



Opsware[®] SAS 6 User's Guide: Server Automation

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.
T + 1 408.744.7300 F +1 408.744.7383 www.opsware.com

Opware SAS Version 6.1

Copyright © 2000-2007 Opware Inc. All Rights Reserved.

Opware Inc. Unpublished Confidential Information. NOT for Redistribution. All Rights Reserved.

Opware is protected by U.S. Patent Nos. 6,658,426, 6,751,702, 6,816,897, 6,763,361 and patents pending.

Opware, SAS Web Client, Model Repository, Data Access Engine, Web Services Data Access Engine, Software Repository, Command Engine, Opware Agent, Model Repository Multimaster Component, and Code Deployment & Rollback are trademarks and service marks of Opware Inc. All other marks mentioned in this document are the property of their respective owners.

Additional proprietary information about third party and open source materials can be found at <http://www.opware.com/support/sas61tpos.pdf>.

Table of Contents

Preface	29
<hr/>	
Contents of this Guide	29
Conventions in this Guide	31
Icons in this Guide	32
Guides in the Documentation Set and Associated Users	33
Opware, Inc. Contact Information	34
Chapter 1: Introduction to Opware SAS	35
<hr/>	
Overview of Opware SAS	35
Types of Opware Users	37
Opware SAS Interfaces and Tools	38
Opware SAS Features	40

Operating System Provisioning	42
Code Deployment & Rollback	43
Configuration Tracking	43
Script Execution	44
Discovery and Agent Deployment.....	45
Device Explorer.....	45
Virtualization Director	46
Visual Application Manager	46
Audit and Remediation	47
Compliance Dashboard.....	47
Reports.....	48
Software Management	48
Patch Management for Windows	48
Patch Management for Unix.....	49
OS Provisioning.....	49
Visual Packager	49
Application Configuration Management.....	50
Global Shell	50
NAS Integration.....	51
Opware SAS Terms and Concepts.....	51
Agent-Server Architecture of Opware Technology	52
Server Management in Multiple Facilities	53
Multimaster Support	55
Chapter 2: Getting Started with the SAS Web Client	57
Getting Started with the SAS Web Client	57

Supported Browsers for the SAS Web Client.....	57
Browser Configuration Requirements	58
Access to Features in the SAS Web Client	58
System Management of Opsware User Information	58
Best Practices for Selecting Passwords.....	59
Updating User Profiles and Passwords	59
User Interface	60
Requirements for Logging In	60
Overview of the SAS Web Client User Interface	60
My Profile.....	68
Search.....	68
My Servers.....	68
Mouseover Icon Tooltips.....	69
 Chapter 3: Getting Started with SAS Client	 71
Overview of the SAS Client	71
Requirements for Running the SAS Client	72
Installing and Launching the SAS Client	72
SAS Client User Interface	75
Menus.....	76
Navigation Pane	77
Search.....	77
Content Pane	78
Details Pane.....	80
Status Bar	82
SAS Client Search	82

Performing a Simple Search.83
Performing an Advanced Search.84
Running a Saved Search Query.86
Deleting a Saved Search.86
Accessing SAS Client Options87
Accessing SAS Client Options.87
General Options87
Unmanaged Servers.88
Packaging Servers91
Terminal and Shell92
Patch Policies94
Visual Application Manager (VAM) Options94
Virtualization Settings94
Scan Time-Out Preference.95
Opsware NAS95
Browsing Job Logs96
Chapter 4: Opsware Agent Management	99
Opsware Agent on Managed Servers99
Overview of the Opsware Agent on Managed Servers.99
Security for Opsware Agents Running on Managed Servers.	101
Opsware Agent Functionality on Managed Servers.	102
Server Information that the Opsware Agent Tracks	103
Opsware Discovery and Agent Deployment.107

Discovering Servers for Installing an Opsware Agent	108
Setting Deployment Actions for Each Server	109
Specifying Login Settings	110
Opsware Agent Installer Options.	110
Reports on Server Status	113
Opsware Agent Installation Using ODAD	115
Prerequisite Setup for Opsware Discovery and Agent Deployment. . .	115
Permissions Required for Opsware Discovery and Agent Deployment	115
Installing Opsware Agents Using ODAD	116
Viewing Unmanaged Server Information	119
Summary Information for an Unmanaged Server.	119
History Information for an Unmanaged Server.	121
Remote Terminal Sessions on Unmanaged Servers	122
Reports on Opsware Agent Installation	123
Agent Reachability Communication Tests	125

Overview of Communication Tests	126
Communication Tests and Unreachable Opsware Agents	126
Communication Test Types	126
Communication Test Errors	128
Additional Information on Communication Tests	133
Running a Communication Test on an Individual Server	133
Running a Communication Test on Multiple Servers	134
Viewing Servers by Communication Status	136
Searching for Unreachable Servers	137
Creating Communication Test DCI Reports	139
Viewing My Jobs Communication Tests	139
Exporting the Unreachable Server Status List to CSV	139

Chapter 5: Exploring Servers and Groups in SAS Client 141

Device Explorer	141
Device Explorer Interface	143
Accessing the Device Explorer	143
Opening a Remote Terminal	144
Server Information	145

Summary	145
Properties.....	146
Hardware	147
File System	148
Installed Packages	151
Configured Applications	151
Software Policies	152
Services	152
Patches.....	153
Patch Policies - Windows Only	156
Patch Contents	156
Windows Registry.....	156
Windows IIS Metabase	157
Windows COM+ Objects	157
Audit and Remediation	158
Custom Attributes	158
Group Membership	158
Server History	159
Compliance	159
Virtualization	160
Device Groups	161

Characteristics of Device Groups	162
Types of Device Groups	163
Public and Private Device Groups	163
Static and Dynamic Device Groups	164
Ways to Create Device Groups	165
Adding a Server to a Static Device Group	169
Adding a Server to a Dynamic Device Group	171
Removing Servers from a Static Device Groups	173
Removing Servers from a Dynamic Group	174
Moving a Device Group	175
Duplicating a Device Group	176
Deleting a Device Group	177
Device Group Explorer	177
Device Group Explorer	179
Accessing the Device Groups Explorer	180
Device Group Explorer Interface	180
Chapter 6: Virtualization Director	185
Virtualization Director Overview	185
Virtualization Director Permissions	186
Key Terms and Concepts	187
Virtualization Director Usage	187

OS Provisioning Virtual Servers – Overview	188
Solaris 10 Local Zone Management Usage Examples	190
Search and Group Virtual Servers	192
Report on Virtual Technologies	192
View Virtual Servers in VAM.	193
Viewing Virtual Servers in the SAS Client	194
View Virtual Server Relationships	194
View Virtual Servers in All Managed Servers List.	196
View Virtual Servers in the Device Explorer	198
View Virtual Server in Reports.	202
Virtual Servers in VAM	204
Viewing Virtual Servers with VAM.	204
Virtual Servers in the SAS Web Client	206
Virtual Server Status	206
Virtual Server States	207
Solaris Local Zone Management	213
Starting and Stopping Local Zones	213
Creating a Local Zone.	214
Modifying a Local Zone.	220
Removing a Local Zone.	223
Searching for Virtual Servers	225
Creating Device Groups for Virtual Servers.	228
Chapter 7: Server Tracking in the SAS Web Client	231
Server Tracking.	231

Ways to Locate, List, and Display Servers	231
Tracked Server Properties	232
Supported Operating Systems for Managed Servers	232
Server Lists	235
Types of Server Lists	235
Server Pool	236
Manage Servers List	237
Filters on the Manage Servers List	238
My Servers	239
Overview of My Servers	239
Adding Servers to My Servers	240
Removing Servers from My Servers	241
Server Search	242
Searching for a Server By Using the Search Box.	242
Ways to Use Search.	243
Using the Search Feature	243
Rules for Server Search and for Creating Dynamic Groups	248
Line Break Workaround for Server Search	257
Conditions for Searching with Multiple Rules	257
Server Searching by IP Address	258
Example: Server Search	258
Searching for a Server Group	259
Server Identification	260

Overview of Server Identification	260
Ways that Servers are Identified by Opsware SAS	261
Customer Accounts in Opsware SAS.....	262
Associating Servers with Customers	264
Server Histories and Reports	267
Overview of Server History.....	267
Viewing Server History	268
Time Stamp for Server Operations.....	269
Hardware Information for Managed Servers	270
Viewing Managed Server Hardware Information	270
Chapter 8: Server Management in SAS Web Client	273
<hr/>	
Overview of Server Management	273
Communication Between Managed Servers and Opsware SAS	275
Network Address Translation (NAT) for Managed Servers.....	275
Key Terms of Opsware SAS Managed Server Communication.....	275
Locating the Management IP Address of a Managed Server	276
Code Deployment and Static NAT	278
Setting the Primary IP Address of a Server.....	278
NAT Table Mapping and Managed Servers.....	279
Server Groups.....	280

Overview of Server Groups	280
Types of Server Groups	283
Public Group Modeling	284
Using Server Groups Tabs	286
Ways to Create Server Groups	288
Adding a Server to Static Groups, Both Public and Private	302
Adding a Server to Dynamic Groups, Both Public and Private	302
Removing Servers from Static Groups, Both Public and Private	303
Removing Servers from Dynamic Groups, Both Public and Private ...	304
Moving Servers from One Static Group to Another	304
Duplicating Server Groups	305
Rules for Deleting Server Groups	307
Server Life Cycle	308
OS Provisioning and the Server Life Cycle	308
Server Properties	316
Server Management Tasks Related to the Server Life Cycle	318
Changing the Use and Stage Values for Servers	320
Editing the Properties of a Server	320
Tasks Associated with Deactivating a Server	322
Deactivating a Server	322
Deleting a Server from Opsware SAS	323
Server Management Jobs	323

My Jobs	324
My Jobs Display Information	324
My Jobs in the Opsware SAS Web Client	326
Jobs in SAS Client	326
Viewing Job Details in the Opsware SAS Web Client	327
Viewing My Job Details from inside the SAS Client	329
Server Management Scheduling and Notification	330
Time-Outs for Server Management Jobs	333
Custom Fields for Servers	334
Overview of Custom Fields for Servers	334
Changing the Value for a Custom Field	335
Custom Attributes for Servers	336
Overview of Custom Attributes for Servers	337
Managing Custom Attributes	337
Adding Server Custom Attributes	338
Editing Server Custom Attributes	339
Deleting Server Custom Attributes	339
Service Levels	340
Overview of Service Levels	340
Adding a Service Level to the SAS Web Client	341
Editing a Service Level	342
Ways to View the Service Level for Servers	342
Assigning a Server to a Service Level	343
Removing a Server from a Service Level	344
Network Configuration	345

Overview of the Server Network Configuration	345
Configuring Networking for an Opsware Managed Server.	346
Chapter 9: NAS Integration	351
Overview of NAS Integration	351
NAS Integration Features	353
How NAS Data is Collected	353
SAS Client Communication	354
Prerequisites	355
Device Information in SAS	355
Viewing Network Interfaces	356
Viewing Network Ports	357
Connections Between Network Devices and Servers.	359
Inferred Physical Connections.	361
Device Groups	362
Associating a NAS Device Group	362
Combined Device History Log.	363
Network Device Information in NAS	369
Viewing a Network Device Directly in Opsware NAS	369
Viewing Event History Directly in Opsware NAS	370
Duplex Mismatch	371
Viewing Duplex Mismatches in the Dashboard	372
Viewing Duplex Mismatches by Server	372
Viewing Duplex Mismatches by Network Device.	372
Network Reports.	372

Chapter 10: Global Shell

375

Overview of the Global Shell	375
Opsware Global File System (OGFS)	375
Remote Opsware Shell (rosh) Utility	376
Benefits of the Global Shell	376
Commands Available in the Global Shell	376
Differences Between the Global Shell and Unix Shells	377
Server Filtering in the OGFS	377
Global Shell Tutorial	379
Global Shell Examples	386
Opening a Global Shell Session	386
Finding Servers in the OGFS	386
Getting Server Information from the OGFS	387
Browsing a Server's File System or Registry	388
Managing Custom Attributes	388
Copying Files Within the OGFS	389
Copying Files Between the OGFS and a Development Server	389
Logging on to a Managed Server With rosh	390
Running OGFS Scripts on Managed Servers With rosh	391
Running Native Programs on Managed Servers With rosh	391
Character Encoding for the OGFS	392

Terminal Application Configuration.....	393
Data that Cannot Be Displayed.....	393
LANG and LC_CTYPE Environment Variables.....	393
Transcoded Data in a Managed Server.....	394
Disabling the Transcoding of Managed Server Data.....	396
Global Shell Error Messages.....	396
Remote Terminal.....	397
Prerequisite for a Remote Terminal.....	397
Opening a Remote Terminal.....	398
Chapter 11: Distributed Script Execution.....	399
Distributed Script Execution.....	399
Overview of Distributed Script Execution.....	399
Scripts Types – My Scripts, Shared Scripts, and Ad-Hoc Scripts.....	400
Script Execution Functionality.....	401
Ways to Initiate Script Operations.....	403
Script Management Tasks.....	404
Viewing the Scripts List.....	408
Editing, Deleting, and Downloading a Script.....	408
Script Version History.....	412
Script Execution.....	412
Overview of Script Execution.....	413
Script Execution Guidelines.....	414
Executing My Script or Shared Scripts.....	414
Creating and Executing an Ad-Hoc Script.....	419
Script Execution Results.....	423

Viewing Execution Results Immediately After Script Execution	425
Viewing Execution Results Stored in Opsware SAS	426
Error Resolution for Script Execution	427
Resolving Script Uploading Errors.	427
Resolving Script Time-out Events	427
Investigating Script Non-Zero Return Codes	428
Investigating Server Authentication Errors	428
Investigating Partial Executions.	428
Opsware SAS Custom Extensions	428
Running a Custom Extension.	429
Chapter 12: Code Deployment and Rollback	435
Opsware Code Deployment Process	435
Deploying Code	435
Uploading Code and Content to Staging.	437
CDR Operations and Directories.	438
CDR Features	439
CDR Permissions	440
Accessing CDR.	441
Services, Synchronizations, and Sequences	442

Overview of Performing Services, Synchronizations, and Sequences .	443
Synchronization of Site Code and Content	443
Performing Synchronizations	445
CDR Cutover Operation	447
CDR Service Operations	449
Starting and Stopping Host Services	449
Backing Up Code and Content	449
Restoring Code and Content from a Previous Version	451
Rolling Back Code and Content to the Previous Version	451
Accessing Service Operations in CDR	452
Performing Service Operations by Service Name	453
Performing Service Operations by Host Name	455
Performing Sequences	457
Processing Code Deployment Requests from Users	459
Status View of Previous Operations	460

Chapter 13: Configuration Tracking 463

Overview of Configuration Tracking	463
File Types Supported	464
Configuration Tracking Operations	464
Change Detection	465
Types of Actions Performed	465
Types of Backups Performed	465
Email Automated Configuration Tracking and Logging Actions	466
Creating the Email Notification List	467
Customized Configuration Tracking Policies	468

Server-Based Entries	469
Policies for Customizing Multiple Servers	469
Adding or Editing Customized Tracking Policy Entries	470
Disabling Customized Tracking Policy Entries	473
Enabling Customized Tracking Policy Entries	474
Viewing a Server's Tracking Policy	474
Reconciling Customized Tracking Policies	475
Enabling and Disabling Configuration Tracking on Servers	475
Manual Backups	477
Performing Manual Backups	477
Backup History	477
Viewing the Backup History	478
Viewing the List of Backup Events	479
Types of Backup Events	479
Backup History Search Options	480
Backup Info and Backup Manifest	480
File Info and File Versions	483
Deleting Backups	484
Restoration of Backed Up Files	485

Overview of Procedures Used to Restore Backed Up Files.....	485
Restore Queue	486
Storing files in the Restore Queue	486
Incremental Backups for Restoration and Rollbacks	486
Entries for Directories in the Backup History	487
File Not Found Entries.....	487
Restoring Backups.....	488
Rolling Back Restored Files	488

Appendix A: Communication Test Troubleshooting **491**

Overview of Agent Communication Tests	491
Command Engine to Agent (AGT).....	492
AGT – OK.....	493
AGT – Untested	493
AGT – Unexpected error.....	493
AGT – Connection refused.....	493
AGT – Connection time-out.....	494
AGT – Request time-out.....	494
AGT – Server never registered	495
AGT – Realm is unreachable	495
AGT – Tunnel setup error.....	496
AGT – Gateway denied access.....	496
AGT – Internal Gateway error	496
AGT – Gateway could not connect to server.....	496
AGT – Gateway time-out	497
Crypto Match (CRP)	497

CRP – OK.....	497
CRP – Untested	497
CRP – Unexpected error.....	497
CRP – Agent certificate mismatch	498
CRP – SSL negotiation failure	498
Agent to Command Engine (CE)	499
CE – OK	499
CE – Untested.....	499
CE – Unexpected error	500
CE – Connection refused	500
CE – Connection time-out	500
CE – DNS does not resolve	501
CE – Old Agent version.....	501
CE – Realm is unreachable	501
CE – No Gateway defined	502
CE – Tunnel setup error	502
CE – Gateway denied access	502
CE – Gateway name resolution error.....	502
CE – Internal Gateway error.....	503
CE – Gateway could not connect to server	503
CE – Gateway time-out.....	503
CE – No callback from Agent	504
Agent to Data Access Engine (DAE).....	504

DAE – OK.....	505
DAE – Untested	505
DAE – Unexpected error.....	505
DAE – Connection refused.....	505
DAE – Connection time-out.....	506
DAE – DNS does not resolve.....	506
DAE – Old Agent version	506
DAE – Realm is unreachable	507
DAE – No Gateway defined	507
DAE – Tunnel setup error	507
DAE – Gateway denied access	508
DAE – Gateway name resolution error	508
DAE – Internal Gateway error	508
DAE – Gateway could not connect to server	508
DAE – Gateway time-out.....	509
Agent to Software Repository (SWR).....	509

SWR – OK	510
SWR – Untested	510
SWR – Unexpected error	510
SWR – Connection refused	510
SWR – Connection time-out	511
SWR – DNS does not resolve	511
SWR – Old Agent version	511
SWR - Server identification error	512
SWR – Realm is unreachable.....	512
SWR – No Gateway defined.....	513
SWR – Tunnel setup error	513
SWR – Gateway denied access.....	513
SWR – Gateway name resolution error	513
SWR – Internal Gateway error.....	514
SWR – Gateway Could not connect to server	514
SWR – Gateway time-out	514
Machine ID Match (MID).....	515
MID – OK	515
MID – Untested	515
MID – Unexpected error	515
MID – MID mismatch	515
Common Troubleshooting Tasks	516

Verifying that an Agent is Running	516
Verifying that a Port is Open on a Managed Server	517
Restarting an Opware Agent	518
Checking Management IP of a Managed Server	518
Checking Network Gateway Configuration	518
Resolving Host Name	519

Appendix B: Opware Agent Utilities **521**

Agent Installation Using the CLI	521
Overview of Agent Installation Using the CLI	522
Preparation for Opware Agent Installation	523
Preassimilation Checklist	524
Installing an Opware Agent by using the Agent Installer CLI	527
Opware Agent Installer Options	528
Starting an Opware Agent on a Server	533
Verifying Opware Agent Functionality	533
Augmenting the Information for a Managed Server	534
Uninstalling an Opware Agent on Unix and Windows	535
Uninstalling Earlier Versions of Opware Agents on Unix	536
Uninstalling Earlier Versions of Opware Agents on Windows	537
Opware Agent Upgrade Tool	538

Ways to Upgrade Opsware Agents.....	538
Prerequisites for Using the Opsware Agent Upgrade Tool.....	539
Upgrading the Opsware Agent on Managed Servers.....	540
Commands for the Opsware Agent Upgrade Tool.....	541
Options for the Opsware Agent Upgrade Tool.....	543
Example: Options for the Opsware Agent Upgrade Tool.....	545
Example: Commands and Output for Agent Upgrade Tool.....	546
Opsware Agent Upgrade Custom Extension.....	546
Upgrading Agents with the Agent Upgrade Custom Extension.....	547
Appendix C: Global Shell Utilities Syntax	553
<hr/>	
aaa Utility.....	553
aaa Syntax.....	553
aaa Usage Rules.....	554
aaa Examples.....	555
Global Shell Operations (Permissions).....	556
rosh Utility.....	558
rosh Syntax.....	558
rosh Usage Rules.....	560
rosh Operations.....	561
rosh Examples.....	561
swenc Utility.....	562
swenc Syntax.....	562
swenc Usage Rules.....	563
Appendix D: OGFS Directories	565
<hr/>	
Directories in the OGFS.....	565

root (/) Directory566
/opsw Directory566
/opsw/Server Directory567
/opsw/Server/@ Directory	568
/opsw/Server/@Facility Directory	570
/opsw/Server/@Group Directory	570
/opsw/Library Directory	571
Other Directories Under /opsw571
/opsw/Application Directory	571
/opsw/Facility Directory	572
/opsw/Group Directory	573
/opsw/Library	574
/opsw/OS Directory	574
/opsw/Permissions Directory	575
/opsw/Realm Directory	576
/opsw/Script/Shared Directory	576
/opsw/ServiceLevel Directory	577
Network Directories577
/opsw/Network Directory	578
/opsw/Network/@Group Directory	579
/opsw/NetModel Directory	579
/opsw/NetOS Directory	580
/opsw/NetType Directory	580
/opsw/Script/Network Directory	580
Appendix E: Glossary	583

Index	599
--------------------	------------

Preface

Welcome to the Opsware Server Automation System (SAS) – an enterprise-class software solution that enables customers to get all the benefits of the Opsware data center automation platform and support services. Opsware SAS provides a core foundation for automating formerly manual tasks associated with the deployment, support, and growth of server and server application infrastructure.

This guide describes how to use Opsware SAS, starting with an introduction to the system and how to navigate the user interface. It provides information about managing servers, operating system provisioning, managing software packages, provisioning applications, managing patches, reconciling servers, script execution, configuration tracking, and deploying and rolling back code. This guide is intended for system administrators who are responsible for all aspects of managing and provisioning the servers in an operational environment.

Contents of this Guide

This guide contains the following chapters and appendices:

Chapter 1: Introduction to Opsware SAS: Provides a high-level overview of Opsware SAS, including the system features, Web Service APIs, and multimaster.

Chapter 2: Getting Started with the SAS Web Client: Includes information about supported operating systems and browsers, navigation of the user interface, and an explanation of each of the features found on the SAS Web Client Home page.

Chapter 3: Getting Started with SAS Client: Includes information about how to get started using the SAS Client, the user interface, the client installation and launch, and SAS Client main features.

Chapter 4: Opsware Agent Management: Includes information about Opsware Agents on managed servers, the Opsware Discovery and Agent Deployment feature, and Opsware Agent reachability communication test.

Chapter 5: Exploring Servers and Jobs in SAS Client: Provides information browsing servers, server groups, and jobs, also includes information about copying files on a managed server's file system.

Chapter 6: Server Tracking in the SAS Web Client: Provides information about server asset tracking, server lists, server search, server histories and reports.

Chapter 7: Server Management in SAS Web Client: Provides information about all aspects of server management including server groups, server life cycle, server locking, and service levels.

Chapter 8: Integration with NAS: Provides information about how you can monitor managed servers and network devices that are connected to them by using Opware Server Automation System (SAS), Opware Network Automation System (NAS), Opware Global Shell, and Opware Visual Application Manager.

Chapter 9: Global Shell: Provides information about the Global Shell, the Opware Global File System, setting user and group permissions with the Global Shell, accessing the Global Shell and remote terminals on servers, and explains Global Shell commands.

Chapter 10: Distributed Script Execution: Describes script types, permissions required for scripting tasks, script version history, and how to create, edit, and delete scripts. It also discusses script execution for all script types, script execution results, and scripting error resolution.

Chapter 11: Code Deployment and Rollback: Provides information about uploading code and content to staging, and performing services, synchronizations, and sequences to deploy code and content to managed servers.

Chapter 12: Configuration Tracking: Provides information about configuration tracking policies, the supported types of configuration files and databases, how changes are detected, and the tracking policies for a specific server. It also discusses reconciling customized tracking policies, performing manual backups, viewing backup history, restoring backed up files, and enabling and disabling configuration tracking.

Appendix A: Communication Test Troubleshooting: Provides troubleshooting information to diagnose Opware Agent unreachable problems.

Appendix B: Opware Agent CLI Utilities: Provides information about installing Opware Agent using the Opware Command Line Interface and the Agent Upgrade Tool.

Appendix C: Global Shell Utilities: Describes the syntax and usage rules for the `aaa`, `rssh`, and `swenc` commands.

Appendix D: OGFS Directories: Provides an overview of the directories under `/opsw`, which can be accessed from within a Global Shell session.

Appendix E: Glossary: Defines terminology and acronyms that are unique to Opware SAS.





Conventions in this Guide

This guide uses the following typographical and formatting conventions.

NOTATION	DESCRIPTION
Bold	Identifies field menu names, menu items, button names, and inline terms that begin with a bullet.
<code>Courier</code>	Identifies text that is entered or displayed at the command-line prompt, such as Unix commands, Opware SAS commands, file names, paths, directories, environment variable names, contents of text files that are viewed or edited with a text editor, source code in a programming language, and SQL (database) commands.
<i>Italics</i>	Identifies document titles, DVD titles, web site addresses. Used to introduce new terms when they are first defined in a document and for emphasis.

Icons in this Guide

This guide uses the following icons.

ICON	DESCRIPTION
	<p>This icon represents a note. It identifies especially important concepts that warrant added emphasis.</p>
	<p>This icon represents a requirement. It identifies a task that must be performed before an action under discussion can be performed.</p>
	<p>This icon represents a tip. It identifies information that can help simplify or clarify tasks.</p>
	<p>This icon represents a warning. It is used to identify significant information that must be read before proceeding.</p>

Guides in the Documentation Set and Associated Users

- The *Opware® SAS User's Guide: Server Automation* is intended for system administrators responsible for all aspects of managing servers in an operational environment. It describes how to use Opware SAS, introducing the system and the user interface. It provides information about managing servers, remediating servers, script execution, configuration tracking, deploying and rolling back code, and agent deployment. It also explains how to use the Opware Global Shell and open a Remote Terminal on managed servers.
- *Opware® SAS User's Guide: Application Automation* is intended for system administrators responsible for performing the day-to-day functions of managing servers. It reviews auditing and compliance, software packaging, visual application management, application configuration, and software and operating system installation on managed servers.
- The *Opware® SAS Administration Guide* is intended for Opware administrators responsible for monitoring and diagnosing the health of the Opware SAS components.
- The *Opware® SAS Deployment and Installation Guide* is intended for advanced system administrators responsible for planning all facets of an Opware SAS installation. It documents all the main features of Opware SAS, scopes out the planning tasks necessary to successfully install Opware SAS, explains how to run the Opware Installer, and details how to configure each of the components. It also includes information on system sizing and checklists for installation.
- The *Opware® SAS Policy Setter's Guide* is intended for system administrators responsible for all facets of configuring the Opware SAS Web Client. It documents how to set up users and groups, how to configure Opware server management, and how to set up the main Opware SAS features, such as patch management, configuration tracking, code deployment, and software management.
- The *Opware® SAS Content Utilities Guide* is intended for advanced system administrators responsible for importing content such as software packages into Opware SAS. It documents the following command-line utilities: OCLI 1.0, IDK, and DET (CBT).
- The *Opware® Automation Platform Developer's Guide* is intended for software developers responsible for customizing, extending, and integrating Opware SAS. It documents how to create Web Services, Java RMI, and CLI clients that invoke methods on the Opware API.

Opware, Inc. Contact Information

The main web site and phone number for Opware, Inc. are as follows:

- <http://www.opware.com/index.htm>
- +1 (408) 744-7300

For links to the latest product documentation and software downloads, see the Opware Customer Support site:

- <https://download.opware.com/opsw/main.htm>

For troubleshooting information, you can search the Opware Knowledge Base at:

- <https://download.opware.com/kb/kbindex.jspa>

The Opware Customer Support email address and phone number are as follows:

- support@opware.com
- +1 (877) 677-9273

Chapter 1: Introduction to Opsware SAS

IN THIS CHAPTER

This section discusses the following topics:

- Overview of Opsware SAS
- Opsware SAS Interfaces and Tools
- Opsware SAS Features
- Opsware SAS Terms and Concepts

Overview of Opsware SAS

Opsware SAS provides a core set of features that automate critical areas of server and application operations – including the provisioning, deployment, patching, and change management of servers – across major operating systems and a wide range of software infrastructure and application products.

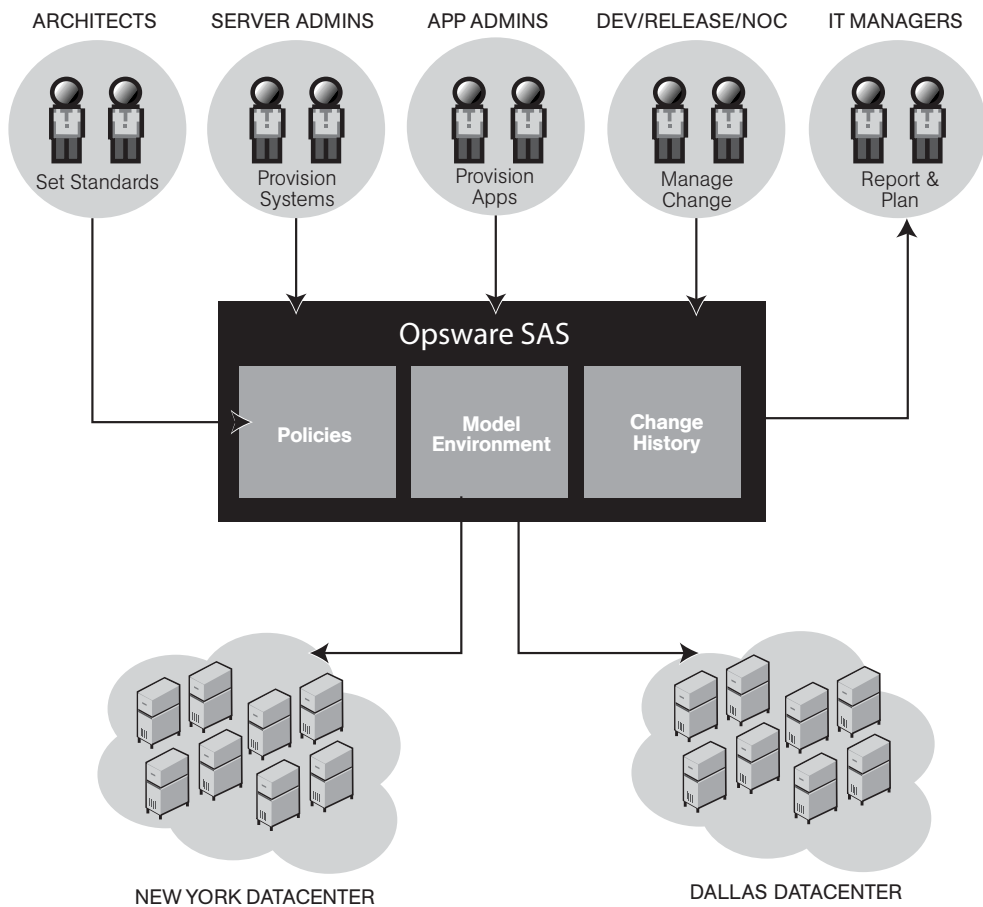
Opsware SAS does not just automate your operations, it also allows you to make changes more safely and consistently, because you can model and validate changes before you actually commit the changes to a server. Opsware SAS helps ensure that modifications to your servers work on your first attempt, thereby reducing the risk of downtime.

Using Opsware SAS, you can coordinate many operations tasks, across many IT groups with everyone working with the same understanding of the state of servers, applications, and configurations. This coordination ensures that all IT administrators have full knowledge of the current state of the environment before further changes are made.

Opsware SAS allows you to incorporate and maintain operational knowledge gained through long hours of trial-and-error processes. After an administrator has found and tested a procedure or configuration, that knowledge can be translated into a model that is stored in a central repository. This allows you to continue to benefit from the operational knowledge gained by your system administrators, even if they are no longer working in your organization.

The following figure provides an overview of how Opware SAS automates server and application operations across all major platforms and a wide range of applications. Each feature that is shown in the diagram is discussed in the following sections.

Figure 1-1: Overview of Opware SAS Features



Types of Opware Users

The following table identifies the types of Opware users and their responsibilities.

Table 1-1: Types of Opware Users

OPSWARE USER	RESPONSIBILITIES
Data Center and Operations Personnel	After manually racking and stacking servers, manage customer facilities and boot bare-metal servers over the network or from an Opware boot image.
System Administrators	Install operating systems and applications (for example, Solaris 5.7 or WebLogic 6.0 Web Server), upgrade servers, create operating system definitions, and set up software management policies.
Site Engineers and Customer Project Managers	Deploy custom code on servers.

In addition to the Opware users listed above, this guide describes the following three types of users:

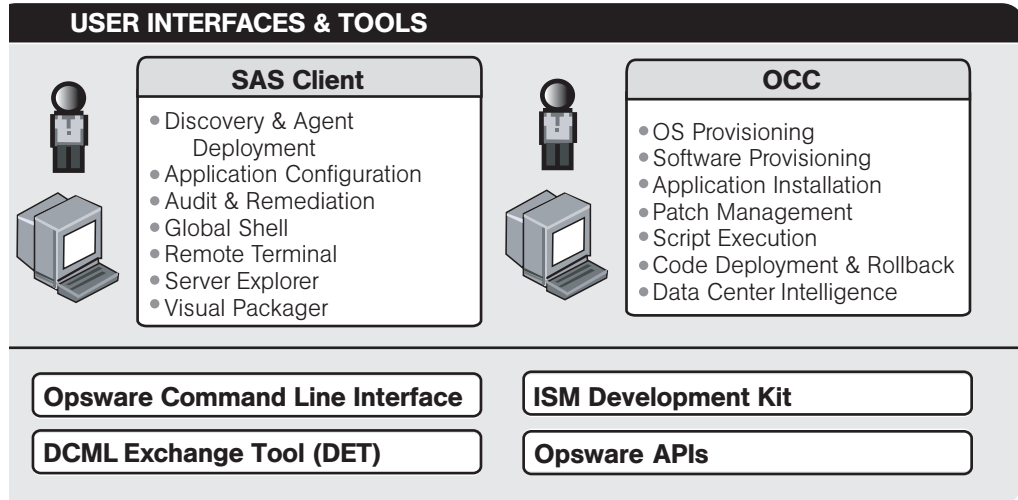
- **End Users** are responsible for all aspects of managing and provisioning the servers in an operational environment. In the Opware SAS documentation, these users are referred to as Opware users or system administrators. These users log into the Opware SAS Web Client and SAS Client and use these interfaces to manage servers in their IT environment.
- **Opware Administrators** are the users, with special training and information, who are responsible for installing and maintaining Opware SAS. In the Opware SAS documentation, these users are referred to as Opware administrators. They use the Administration features in the SAS Web Client to manage Opware SAS and Opware users (by adding user accounts and assigning permissions for different levels of operation and access), to add customers and facilities, and to change Opware SAS configurations. They monitor and diagnose the health of Opware SAS components. Opware administrators need to understand how Opware SAS features operate to support users and Opware SAS.
- **Policy Setters** are the power users who are responsible for architecting what Opware SAS will do in the managed environment; for example, they determine which operating systems can be installed on your managed servers and how those operating systems

will be configured during installation. Policy setters, for example, prepare specific features in Opware SAS by defining the Software Policies, preparing Operating System Definitions, and acting as Patch Administrators to approve patches for installation in the operational environment.

Opware SAS Interfaces and Tools

Depending on the type of operation you need to perform with Opware SAS, you select the appropriate user interface, as Figure 1-2 shows.

Figure 1-2: Interfaces in Opware SAS



- **Opware SAS Web Client:** The web-based user interface to Opware SAS through which users can manage servers, provision applications and operation systems onto servers, run distributed scripts on servers, and deploy code and content to servers, among other things.
- **SAS Client:** A Java Web-Start application that extends the SAS Web Client features and provides the following new features:
 - Discovery and Agent Deployment
 - Device Explorer
 - Virtualization Director
 - Visual Application Manager
 - Audit and Remediation

- Compliance Dashboard
 - Reports
 - Software Management
 - Patch Management for Windows
 - Patch Management for Unix
 - Visual Packager
 - Visual Packager
 - Application Configuration Management
 - Global Shell
 - NAS Integration
- **Opsware Command Line Interface (OCLI):** A command line interface that users can use to upload packages to the Opsware Software Repository (version 1), and perform many other Opsware SAS operations (version 2).
 - **DCML Exchange Tool (DET):** A utility that enables users to export almost all server management content from any Opsware core – standalone or multimaster mesh – and import it into any other Opsware core. Opsware SAS can also provide pre-packaged server management content appropriate for new installations that can be imported into a core after initial setup. See the *Opsware® SAS Content Utilities Guide* for information about using this utility.
 - **ISM Development Kit:** A development kit that consists of command-line tools and libraries for creating, building, and uploading ISMs. An ISM is a set of files and directories that include application bits, installation scripts, and control scripts. See the *Opsware® SAS Content Utilities Guide* for information about using the ISM Development Kit.
 - **Opsware APIs:** A set of APIs and a command-line interface (CLI) that facilitate the integration and extension of Opsware SAS. This platform allows other IT systems – such as existing monitoring, trouble ticketing, billing, and virtualization technology – to exchange information with Opsware SAS. This broadens the scope of how IT can use Opsware SAS to achieve operational goals.

Opsware SAS Features

Opsware SAS is made up of a set of Opsware SAS features. Opsware SAS features are the components that automate particular IT processes.

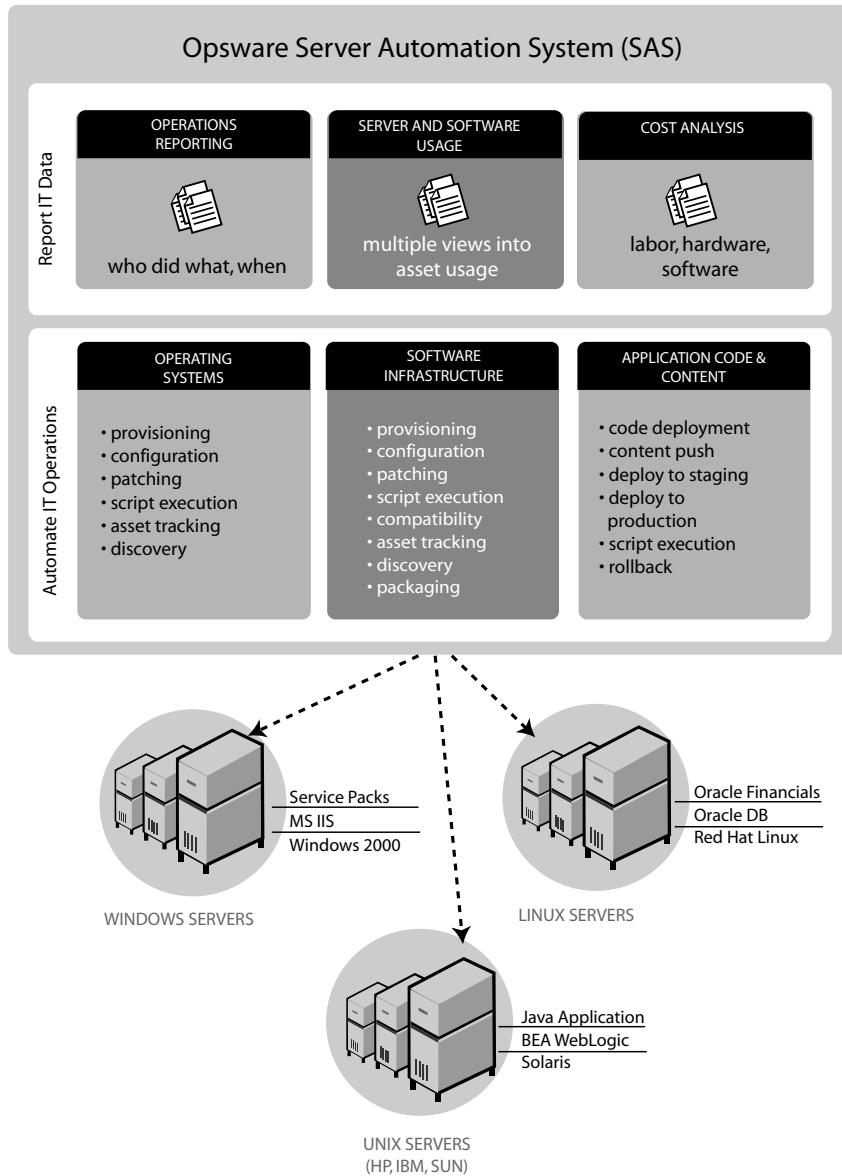
The features are designed to replace ad hoc, error-prone, manual processes. For example, by using the OS Provisioning feature, users can set standards for different types of servers and automatically provision the servers, saving time and ensuring that operating system builds are consistent. By using the Patch Management feature, users can establish policies about how patches are installed. Opsware SAS uniformly enforces those policies.

The following features are currently available as part of Opsware SAS:

- Operating System Provisioning
- Code Deployment & Rollback
- Configuration Tracking
- Script Execution
- Discovery and Agent Deployment
- Device Explorer
- Virtualization Director
- Visual Application Manager
- Audit and Remediation
- Compliance Dashboard
- Reports
- Software Management
- Patch Management for Windows
- Patch Management for Unix
- OS Provisioning
- Visual Packager
- Application Configuration Management
- Global Shell
- NAS Integration

All Opware SAS features support cross-platform environments and are designed to automate both new and existing data center environments. See the following figure.

Figure 1-3: Opware SAS Features



Operating System Provisioning

The OS Provisioning feature gives administrators the ability to provision operating system baselines onto bare metal servers quickly, consistently, and with minimal manual intervention. Bare metal OS provisioning is a key part of the overall process of getting a server into production.

Benefits of the OS Provisioning feature include the following items:

- **Integration with the other features of Opsware SAS**

Because the OS Provisioning feature is integrated with the suite of Opsware SAS automation capabilities, including patch management, software management, and distributed script execution, handoffs between IT groups are seamless. Opsware SAS ensures that all IT groups are working with a shared understanding of the current state of the environment, which is an essential element of delivering high-quality operations and reliable change management.

- **The ability to easily update server baselines without re-imaging servers**

Unlike many other OS provisioning solutions, systems provisioned with Opsware SAS can be easily changed after provisioning to adapt to new requirements. The key to this benefit is the Opsware SAS use of templates and its installation-based approach to provisioning.

- **Flexible architecture designed to work in many environments**

Opsware engineers carefully designed the OS Provisioning feature to handle many different types of servers, networks, security architectures, and operational processes. Opsware SAS works well in floppy (Windows provisioning), CD (Linux provisioning), or network-boot environments, with scheduled or on-demand workflows, and across a large variety of hardware models. This flexibility ensures that you can provision operating systems to suit your organization's needs.

Opsware SAS automates the entire process of provisioning a comprehensive server baseline, which typically consists of the following tasks:

- Preparing the hardware for OS installation using an OS installation profile
- Creating OS sequences that define a server build policy, including application policies, patch policies, device groups, and remediation policies
- Installing a base operating system and default OS configuration using an OS sequence

- Applying the latest set of OS patches, the exact list depends on the applications running on the server
- Installing system agents and utilities such as SSH, PC Anywhere, backup agents, monitoring agents, or anti-virus software
- Installing widely-shared system software such as Java Virtual Machines
- Executing pre-installation or post-installation scripts that configure the system with values such as a root password

Code Deployment & Rollback

Opsware SAS automates code and content deployment to reduce the risk and time requirements associated with pushing new code to production. The Code Deployment & Rollback (CDR) feature provides an automated system for deploying code (such as, ASP, JSP, JAR, Java, C++, and Perl files) and content (such as, HTML, JPEG, GIF, and PDF files).

Specifically, CDR enables you to perform the following actions:

- Push code from staging or development environments to production environments.
- Synchronize code and content across multiple servers and locations.
- Automatically rollback to the previous version of code or content.
- Sequence multiple, complex deployment steps into repeatable workflows.
- Manage changes across heterogeneous operating systems.

Configuration Tracking

The Configuration Tracking feature tracks, backs up, and recovers critical software and system configuration information across Unix and Windows servers.

System administrators set up policies that describe the configuration files and databases to track, and the actions to take when a change in configuration is detected. Policies can be assigned to software, individual servers, groups of servers, and customers, and applied either locally or globally across data centers.

When Opsware SAS notices a server configuration change, it can log the change, notify administrators about the change with email, or back up the configuration, depending on the policy set by the administrator.

When a bad configuration change forces administrators to rollback to a previous version, they can use Opsware SAS to restore the configuration file to the saved version of the configuration. By notifying users about configuration changes – and maintaining a version history of those changes – organizations can quickly diagnose problems related to configuration errors and rollback to a known good state. In addition, this capability helps teams plug security holes inadvertently created by bad server configurations.

Typically, system administrators define configuration-tracking policies on a per-application basis. So for example, a policy for BEA WebLogic might specify, “Monitor the `weblogic.conf` file, notify `app-server-admins@company.com` of any changes, and maintain a version history of any changes that occur for 30 days.” After a policy is defined in this fashion, administrators can apply the policy to all the WebLogic servers running in their environment or to specific servers.

Script Execution

The Script Execution feature enables you to share and run ad-hoc or custom scripts across an entire farm of Opsware-managed servers.

By executing scripts with Opsware SAS instead of manually, administrators benefit by using the following features:

- Parallel script execution across many Unix and/or Windows servers, saving time and ensuring consistency.
- Role-based access control, ensuring only authorized administrators can execute scripts on hosts to which they have access.
- The ability to control access to scripts by storing them in private or in public libraries.
- The ability to see and download script output one server at a time or in a consolidated report, which captures output from all servers in a single place.
- The ability for scripts to be mass-customized. Administrators can access information in Opsware SAS about the environment and the state of servers. This is critical to ensuring that the right scripts are executed on the right servers.
- A comprehensive audit trail that reports who, what, when, and where a particular script was executed.
- The ability to rollback changes (when used in conjunction with the Configuration Tracking feature).

- Automatic backup of all private and shared scripts to all other Opsware-managed data centers (when used in conjunction with an Opsware Multimaster Mesh).

Because the Script Execution feature is an integrated part of Opsware SAS, administrators enjoy unique benefits when compared to standalone script execution tools:

- Using known system state and configuration information to customize script execution, users can tailor each script by referencing and accessing the rich store of information in Opsware SAS, such as the customer or business that owns the server, whether the server is a staging or production server, which facility the server is located in, and custom name-value pairs.
- By sharing scripts without compromised security, users can share scripts with each other without compromising security because Opsware SAS maintains strict controls on who can execute scripts on which servers and generates a comprehensive audit trail of script execution.

Discovery and Agent Deployment

The Opsware Discovery and Agent Deployment (ODAD) feature allows you to deploy Opsware Agents to a large number of servers in your facility and place them under Opsware management.

Using the ODAD features, you can perform the following tasks:

- Scan your network for servers.
- Select servers for Opsware Agent installation.
- Select a communication tool and provide user/password combinations.
- Choose agent installation options and deploy agents.

Device Explorer

The Device Explorer lets you view information about servers in your managed environment.

From the Server Explorer, you can perform the following tasks:

- Create a server snapshot, perform a server audit, audit application configurations, create a package, and open a remote terminal session on a remote server.
- Browse a server's file system, registry, hardware inventory, software and patch lists, and services.

- Browse Opware information such as properties, configurable applications, and even server history.

From the Groups Browser, you can perform the following tasks:

- Audit system information, take a server snapshot, and configure applications.
- View and access group members (servers and other groups).
- View group summary and history information.

Virtualization Director

The Virtualization Director feature enables you to provision and manage virtual servers for Solaris 10 local zones and VMware ESX 3 virtual machines (VMs). Using the SAS Client, you can perform the following tasks:

- View both hypervisor and virtual servers and their relationships in the SAS Client, so you can find out the hypervisors that are hosting your virtual machines and local zones.
- View virtual servers and their relationship in the Visual Application Manager (VAM).
- Provision VMware ESX and Solaris 10 hypervisors on bare metal servers.
- Provision VMware virtual machines (VM) using an OS sequence.
- Create, start, stop, modify, and remove Solaris local zones.
- Deploy agents on unmanaged virtual servers using the Opware Agent Discovery and Deployment (ODAD) for VMware ESX VMs.
- Search for virtual servers in your data center using the Search tool.
- Create dynamic Device Groups based upon virtual server characteristics (zones or VMs).

Visual Application Manager

The Visual Application Manager feature is designed to help you optimally understand and manage the operational architecture and behavior of distributed business applications in your IT environment. Since these applications are complex collections of services that typically run across many servers and network devices, it can become increasingly difficult to understand (or remember) what is connected to what, where performance problems originate, how to troubleshoot and resolve problems, and what result would occur if you make a change in your environment.

Visual Application Manager helps you see (visualize) this type of information in physical and logical drawings

Audit and Remediation

The Opware Server Compliance feature allows you to define server configuration policies and make sure that servers in your facilities meet those policy standards. When servers are found to be 'out of compliance' (not configured the way you want them to be), you can remediate the differing server configurations.

With Server Compliance, you can audit a server configuration values based upon a live server (or server snapshot), or based upon your own custom values, perform server comparisons against a baseline, and create custom audit policies that define company or industry server configuration compliance standards, and which can be used inside of audits, snapshot specifications, and audit policies.

Using Server Compliance, you can perform the following tasks:

- Compare servers or snapshots to reference servers or snapshots
- Create audits for repeated use
- Create audit policies that define compliance and security standards for your organization
- Associate audits with individual servers or dynamic server groups
- Remediate problems at multiple levels, including files, directories, patches, registry keys, and packages

Compliance Dashboard

The Compliance Dashboard allows you to view at a glance the overall compliance levels for all the devices in you facility and helps you to remediate compliance problems. The Compliance Dashboard displays compliance tests for software policies, application configurations, audits, patches, and duplex status. Each of these compliance tests is based upon an Opware Server Automation System (SAS) "policy" (user or system defined) which define a unique set up server or device configuration settings or values that help ensure your IT environment is configured the way you want it to be.

Reports

The Reports feature provides comprehensive, real-time information about managed servers, network devices, software, patches, customers, facilities, operating systems, compliance policies, and users and security in your environment. These reports are presented in graphical and tabular format, and are actionable—where you can perform appropriate actions on objects, such as a policy or an audit, within the report. These reports are also exportable to your local file system (in .html and .xls formats) to facilitate use within your organization.

Software Management

The Software Management feature in Opsware SAS provides a powerful mechanism to model software by using software policies and to automate the process of deploying software and configuring applications on a server in a single step. In addition, the Software Management feature provides a structure to organize your software resources in folders and define security permissions around them. This feature allows you to verify the compliance status of a server and remediate non-compliant servers.

The Software Management feature in SAS Client provides the following functions:

- Create an organizational structure for software
- Define security boundaries for folders
- Define a model-based approach to manage the IT environment in your organization
- Enable sharing of software resources among user groups
- Deploy and configure applications simultaneously
- Deploy multiple application instances on one server
- Establish a software deployment process
- Verify compliance status of servers to software policies
- Generate reports
- Comprehensively search for software resources and servers

Patch Management for Windows

The Patch Management for Windows feature enables you to identify, install, and remove Microsoft® Windows patches and maintain a high level of security across managed servers in your organization. With SAS Client user interface, you can identify and install

patches that support security vulnerabilities for the Windows 2000, Windows 2003, and Windows NT4.0 operating systems. These patches include Service Packs, Update Rollups, and hotfixes.

Patch Management for Unix

The Patch Management for Unix feature enables you to identify, install, and remove Unix patches to maintain a high level of security across managed servers in your organization. With the Opware SAS Client, you can identify and install patches that support security vulnerabilities for the AIX, HP-UX, and Solaris operating systems.

OS Provisioning

OS Provisioning in the SAS Client allows you to install an operating system, applications, and packages on unprovisioned servers by creating OS Installation Profiles and OS Sequences. From the Devices list, you can view all unprovisioned servers in your facility and provision those servers by running an OS Sequence.

OS Sequences allow you to set up a complete server build (policy) that represents the ideal manner in which a particular OS should be installed, which includes the proper OS Installation Profile that should be used, as well as Application and Patch policies, the servers to install the OS on, and how these policies should be remediate either before or after the OS is installed.

Visual Packager

The Create Package feature allows you to create an installable software package from a managed server and from server compliance information, such as server snapshots and audit results. File system objects that are recorded in snapshots and compliance information produced by audits help you define the content of a package. In turn, you can use that package to update a server with new or missing server objects.

Create Package enables you to selectively package server objects according to the operating system of the servers that you want to distribute the package to, supporting both Unix and Windows operating systems.

It allows packages to contain the following objects:

- A Unix package can contain files (including attributes), directories, packages, patches, and patch clusters.
- A Windows package can contain files (including attributes), directories, packages, patches, Windows registry, and Windows services.

Application Configuration Management

Opware Application Configuration Management (ACM) allows you to create templates so you can modify and manage application configurations associated with server applications. ACM enables you to manage, update, and modify those configurations from a central location, ensuring that applications in your facility are accurately and consistently configured.

Using ACM, you can perform the following tasks:

- Manage configurations based on files and objects, such as Windows registry, IIS metabase, WebSphere, COM+, and more.
- Preview configuration changes before applying them.
- Edit and push configuration changes to individual servers or server groups.
- Use information in the Opware data model to set configuration values.
- Manage configurations of any application by building configuration templates.
- Audit the Application Configurations on a server to determine if any of the configuration files on the server are out of sync with the values stored in your templates.

Global Shell

The Opware Global Shell feature enables you to manage servers by using a command-line interface. You can remotely perform the following tasks:

- Complete routine maintenance tasks on managed servers.
- Troubleshoot, identify, and remediate problems on managed servers.

Global Shell consists of a file system and a command-line interface to that file system for managing servers in Opware SAS. The file system is known as the Opware Global File System (OGFS). All object types in the OGFS (such as servers, customers, and facilities) are represented as directory structures in this file system.

The Global Shell feature also manages user permissions for accessing the file system, Windows Registry, and Windows Services objects on managed servers.

NAS Integration

The NAS Integration feature enables you to closely examine detailed information about managed servers and the network devices connected to them so that you can determine how they are related and then, subsequently, coordinate and implement those changes. This feature supports an integrated approach to using NAS and SAS so that you can perform actions on device groups, such as combine event history, determine compliance, and identify duplex mismatches across servers and network devices in your environment.

Opsware SAS Terms and Concepts

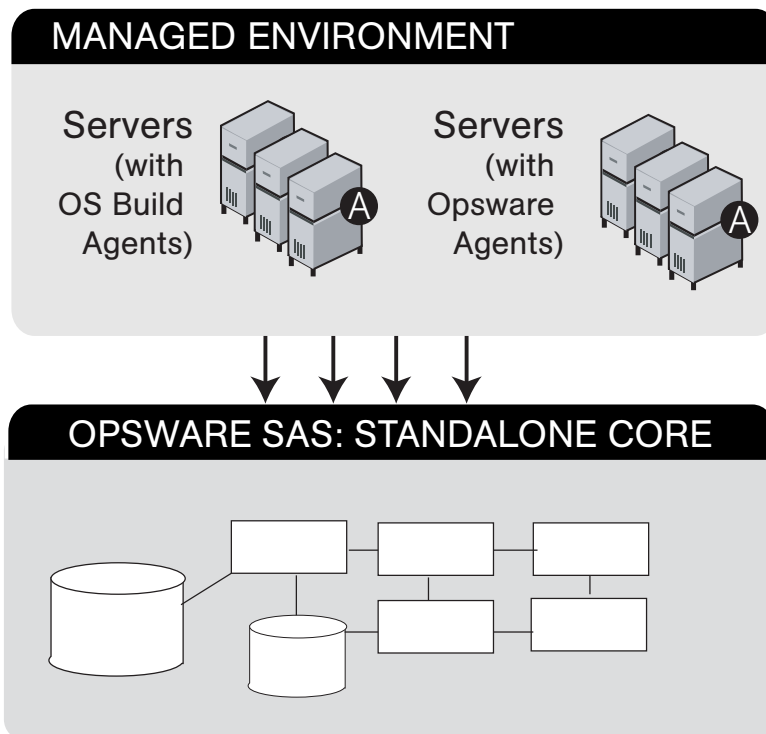
This section discusses the following topics:

- Agent-Server Architecture of Opsware Technology
- Server Management in Multiple Facilities
- Multimaster Support

Agent-Server Architecture of Opware Technology

The agent-server architecture of Opware SAS enables server management. The server portion of Opware SAS consists of multiple, integrated components, each with a unique purpose. Each server managed by Opware SAS runs an intelligent agent (the Opware Agent).

Figure 1-4: Opware SAS Agent-Server Architecture



See the *Opware® SAS Administration Guide* for a detailed description of the components that make up the Opware SAS server portion of the architecture.

The Opware Agent is the agent of change on a server. Whenever Opware SAS needs to make changes to servers, it does so by sending requests to the Opware Agents. Depending on the request, the Opware Agent on a server might use global Opware SAS services in order to fulfill the request. For example, the Opware Agent might often make requests to the Model Repository, the central database for all Opware SAS components, and the Software Repository, the central repository for all software that Opware SAS manages.

Some functions that the Opsware Agent supports are:

- Software installation and removal
- Configuration of software and hardware
- Periodically reporting server status
- Auditing of the server

An Opsware Agent is idle unless Opsware SAS is trying to perform some change on the server. In addition, each Opsware Agent periodically contacts the Data Access Engine and registers itself. The Data Access Engine is an XML-RPC interface to the model repository. The Data Access Engine sends this data to the Model Repository, which allows the Model Repository to keep track of server status, and know when particular servers are disconnected from or reconnected to the network.

After you install an Opsware Agent on a server, users can manage the server by installing or upgrading software, patching the OS software, removing software, changing server properties, or decommissioning the server.

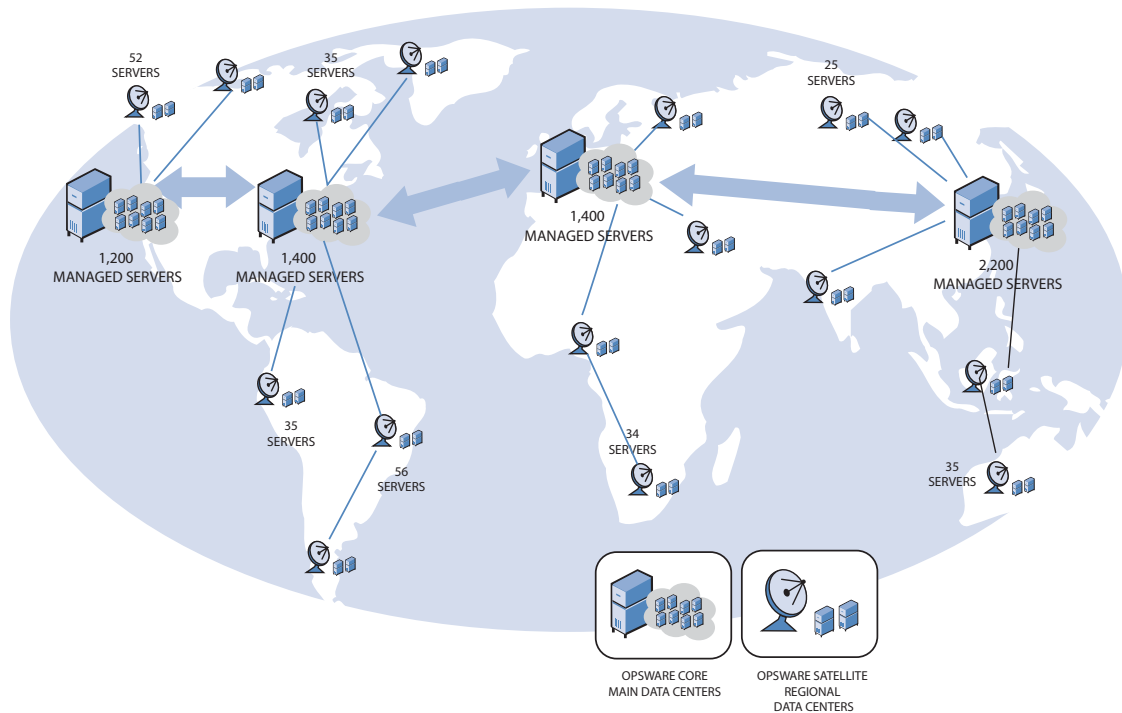
See "Agent Reachability Communication Tests" on page 125 in Appendix for information about how to install an Opsware Agent on a server so that Opsware SAS can manage it.

Server Management in Multiple Facilities

The managed environment might span several facilities. A facility refers to the collection of servers that a single Opsware Model Repository manages, and the database that stores information about the managed environment. For example, one facility might be

dedicated to an organization's Intranet, while another facility might be dedicated to the web services offered to the public. Your Opware SAS can contain facilities (a full Opware SAS is installed) and Satellite facilities. See Figure 1-5.

Figure 1-5: Server Management in Multiple Facilities



See the *Opware® SAS Planning and Installation Guide* for more information about the types of installations that Opware SAS supports.

Users can manage servers in any facility from an SAS Web Client in any facility. When a user updates data in a facility, the Model Repository for that facility is synchronized with the Model Repositories located in all remote facilities.

When using Opware technology in multiple facilities, users should follow these work process rules to reduce the chance of data conflicts between facilities:

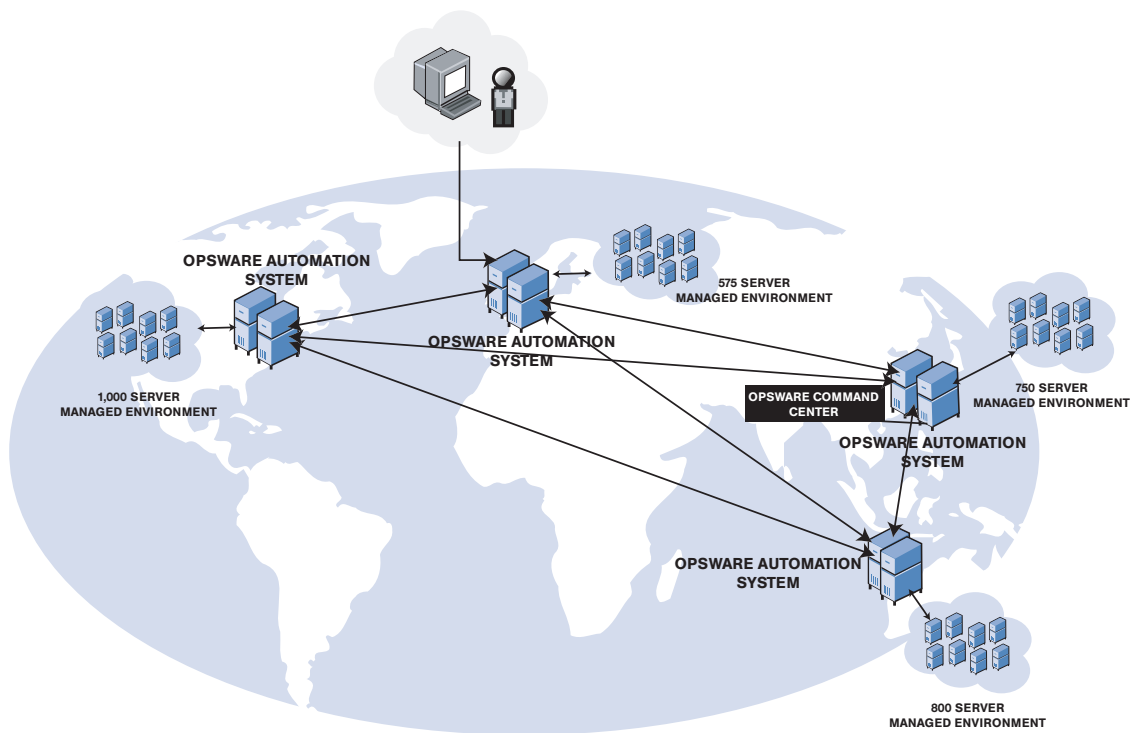
- Users should not change data in one facility and then make the same change in another facility.
- More than one user should not change the same object in different facilities at the same time. For example, two users should not manage the same server from different facilities.

Multimaster Support

With the Opware Model Repository Multimaster Component, customers can store and maintain a blueprint of software and environment characteristics of each data center (referred to as a facility in the Opware SAS Web Client) in multiple locations so the infrastructure can be easily rebuilt in the event of a disaster. The Multimaster Replication Engine not only provides the ability to replicate an environment in case of a disaster, but can also assist in facility migration activities as well as knowledge sharing across the enterprise.

Through the Model Repository Multimaster Component, Opware SAS provides the ability to easily rebuild server and application environments, provision additional capacity, distribute updates, and share software builds, templates and dependencies – across multiple facilities and from one user interface. See Figure 1-6.

Figure 1-6: Multimaster Support



Chapter 2: Getting Started with the SAS Web Client

IN THIS CHAPTER

This section provides an overview of the SAS Web Client and discusses the following topics:

- Getting Started with the SAS Web Client
- Access to Features in the SAS Web Client
- User Interface

Getting Started with the SAS Web Client

The following section describes Supported Browsers for the SAS Web Client (a web application) and Browser Configuration Requirements.

Supported Browsers for the SAS Web Client

The following table lists the supported browsers for the SAS Web Client.

Table 2-1: Supported Browsers for the SAS Web Client

BROWSER	WINDOWS 2000	WINDOWS 2003	WINDOWS XP	LINUX 6.2+	SOLARIS 6 +	MAC OS X
Microsoft Internet Explorer 5.5	X					
Microsoft Internet Explorer 6.0	X	X	X			
Mozilla 1.6	X	X	X			

Table 2-1: Supported Browsers for the SAS Web Client

BROWSER	WINDOWS 2000	WINDOWS 2003	WINDOWS XP	LINUX 6.2+	SOLARIS 6 +	MAC OS X
Firefox 1.0	X	X	X			

Browser Configuration Requirements

To use the SAS Web Client, your browser must be configured in the following manner:

- The browser must accept cookies and be able to use Java.
- The browser must support SSL and should provide 128-bit encryption (recommended).
- Using a pop-up blocker might prevent some functions from working correctly. Either disable the pop-up blocker completely or use the supported browser's native pop-up blocking function instead of a third-party product.

Access to Features in the SAS Web Client

This section explains how to configure your user profile to access features within the Opware System. This section contains the following topics:

- System Management of Opware User Information
- Best Practices for Selecting Passwords
- Updating User Profiles and Passwords

System Management of Opware User Information

An Opware administrator creates additional users who can use the SAS Web Client, and the Opware administrator assigns them temporary passwords. Once added to the system, an Opware user can update their personal information, password, and time zone and date display preferences by using the My Profile link.

An Opware user cannot change their access permissions by using the My Profile link. If an Opware user needs additional access permissions, they contact their Opware administrator.

Best Practices for Selecting Passwords

The Opsware Server Automation System (SAS) enforces a security policy that allows only authorized users to log into the SAS Web Client. Opsware users are advised to select a password based on the following guidelines:

- Change your password frequently to ensure that your account information is secure.
- Select a password that is easy to remember so that you don't have to write it down.
- Use a mixture of upper and lower case letters, numbers, and punctuation in your password.
- Do not share your password.
- Do use a password that you can type quickly, without having to look at the keyboard.

Updating User Profiles and Passwords

As an Opsware user you can change your name, contact information, password, and preferences such as time zone and date display. You cannot change your access permissions. Contact your Opsware administrator to change your access permissions.

Perform the following steps to change your profile and password.

- 1** Log into the SAS Web Client. The SAS Web Client Home Page appears.
- 2** Click the My Profile link located at the top of the page. The My Profile Page appears.
- 3** To change your profile information, enter new information on the User Identification tab of the My Profile Page.
- 4** Click **Save**.
- 5** To change your password, click the Change Password Link. The Password Change page appears.
- 6** Enter your old password.
- 7** Enter your new password.
- 8** Confirm your new password in the Confirm Password field.
- 9** Click **Save**. A confirmation page appears indicating that your password was successfully changed.
- 10** Click **Okay**. The Profile page appears.

User Interface

The following section discusses getting started with the Opware System and contains the following topics:

- Requirements for Logging In
- Overview of the SAS Web Client User Interface
- My Profile
- Search
- My Servers
- Mouseover Icon Tooltips

Requirements for Logging In

In order to log in and access SAS Web Client features, your Opware administrator must have created a user name and password for you, and assigned user permissions that control the features you can access, the actions you can perform, and the resources you can access.

Overview of the SAS Web Client User Interface

The SAS Web Client user interface consists of the five following sections:

- Home Page
- Tasks
- My Jobs
- My Customers
- Navigation Panel

Home Page

Figure 2-1 shows the Home page as it appears when you log in or when you click the Home link in the navigation bar.

Figure 2-1: Opware System Home Page

The screenshot shows the Opware System Home Page. At the top, there is a navigation bar with a search field and a clock showing 17:59 UTC. The left sidebar contains a navigation menu with categories like Home, My Jobs, Servers, Software, Environment, and Administration. The main content area is titled 'Home' and contains three sections:

- Tasks:** A table with three columns: OS Provisioning (Prepare OS), Software Provisioning (Deploy Code), and Power Tools (Launch Opware SAS Client, Run Distributed Script, Run Custom Extension, View Reports).
- My Jobs:** A table with columns: Name, Start Time, Servers, Groups, and Status. One job is listed: 'Remediate Policies' with a start time of 'Tue Aug 01 17:58:52 2006', 1 server, 0 groups, and a status of 'Completed'.
- My Customers:** A table with columns: Customer, Unreachable Servers, and Total Servers. Below the table, it says 'No Customers selected'.



The time zone that appears in the upper right corner of the Home page is taken from the time zone preference that was defined for you when your profile was created.

Consequently, the date and time information that displays throughout the SAS Web Client is for that time zone. The occasional exceptions however are always labeled GMT.

Tasks

The Tasks area of the Home page displays links to the wizards that you have permissions to access, a link to the Code Deployment page if you have that permission. If you do not have permissions to a task in this area, the task name still displays, but it is italicized and it is not an active link. Figure 2-2 shows the Tasks area with all permissions enabled.

Figure 2-2: Tasks Area of the Home Page

Tasks		
OS Provisioning	Software Provisioning	Power Tools
Prepare OS	<i>Deploy Code</i>	Launch Opware SAS Client
		Run Distributed Script
		Run Custom Extensions

My Jobs

The My Jobs area of the Home page is populated with details of the jobs that you have run, jobs that are currently in progress, or jobs that you have scheduled to run, including the name of the job, the start time, the number of servers affected by the job, and the status of the job. If there are more than six jobs, you can see the rest of them by clicking the See All link, which also shows the total number of jobs in parentheses, as Figure 2-3 shows.

If the job was run in the SAS Client, then there will be a link next to the job that (when clicked) will launch the SAS Client. You can view the more detailed information about the job in the SAS Client.

Figure 2-3: My Jobs Area of the Home Page

My Jobs ?






2 Total

	Job ID	Job Type	Start Time ↑	Servers	Groups	Status
	260003	Communication Test	Tue May 17 20:46:35 2005	1	0	Completed
	250003	Communication Test	Tue May 17 20:43:50 2005	1	0	Completed

My Customers

The My Customers area of the Home page is populated with customer information, including unreachable servers associated with a customer and the total number of servers associated with that customer. To select the customers to display in the My Customers area of the Home page, click **Edit** and select the check box next to the customer name. See Figure 2-4.

Figure 2-4: My Customers Area of the Home Page

My Customers			Edit
Customer	Unreachable Servers	Total Servers	
 Arnold	0	0	
 Industrial Machines	0	0	
 MASTERCUST	106	110	
 Opsware	13	23	
 OPSWINC	0	0	

Navigation Panel

The navigation panel on the left side of the SAS Web Client shows all possible features, as shown in Figure 2-5. The features you can access and the actions you can perform depend upon your user profile, as defined by the Opware administrator.

Figure 2-5: Navigation Panel, All Permissions View



The items that appear in the navigation panel depend on the permissions the user has. Clicking an item on the navigation panel displays that feature in the main part of the Home page. For a user with all permissions, the following links appear:

Home: Displays the top level of the SAS Web Client. The Home page is described in this section of the guide. Wizards are documented in their respective functional areas of the system.

My Jobs: Displays the My Jobs page, showing jobs completed during the previous 30 days, jobs currently in progress, and currently scheduled jobs. This page is an expanded view of the contents of the My Jobs area of the Home page and has the same effect as clicking **Show All** in the My Jobs area of the Home page.

Servers: Expands to display these selections:

- **My Servers:** Use to add any server or server group to your own personal view of servers. My Servers provides an efficient way to manage servers when your operational environment contains hundreds or thousands of servers.
- **Manage Servers:** Use filters to display a list of servers and perform operations on them such as edit server values, assign, run scripts, and add servers to My Servers. See “Server Management in SAS Web Client” on page 273 in Chapter 8 for more information.
- **Search:** Find specific servers using default criteria or user-defined criteria. See “Server Search” on page 242 in Chapter 7 for more information.
- **Server Pool:** Use filters to display a list of servers, install operating systems on the servers, and delete the servers. See *Opware® SAS User's Guide: Application Automation* for more information.

Software expands to display these selections:

- **Operating Systems:** Prepare operating systems for installation and delete existing operating systems. See *Opware® SAS User's Guide: Application Automation* for more information.
- **Scripts:** Run scripts, upload scripts, and create new scripts. See “Distributed Script Execution” on page 399 in Chapter 11 for more information.

Environment expands to display these selections:

- **Customers:** Create new customers and edit or delete existing customers. See the *Opware® SAS Administration Guide*.
- **Facilities:** Create new facilities, edit facility properties, and assign and edit custom attributes for facilities. See the *Opware® SAS Planning and Installation Guide*.

- **Hardware:** A read-only view of servers categorized by the hardware manufacturer and model, and their related information. See “Hardware Information for Managed Servers” on page 270 in Chapter 7 for more information.
- **Service Levels:** Define service levels and custom attributes. See “Service Levels” on page 340 in Chapter 8 for more information.
- **IP Ranges:** Identify and create IP ranges and IP range types. See the *Opware® SAS Policy Setter's Guide* for more information.
- **IP Range Groups:** Create IP Range Groups. See the *Opware® SAS Policy Setter's Guide* for more information.

Code Deployment expands to display these selections:

- **Deployment Home:** The exact CDR links that you see in the Code Deployment area are based on the permissions that you have for the customer you want to work with.
- **Service Management:** Create, modify, and delete service definitions. Services define the location and commands to manipulate applications on hosts.
- **Run Service:** Perform service operations on one or more hosts, or request that a service operation be performed on your behalf. Service operations include starting or stopping applications, cutting over or rolling back code, and backing up or restoring code.
- **Sync Management:** Create, modify, and delete synchronization definitions. Synchronizations define the path for pushing code from a source host to one or more destination hosts.
- **Synchronize:** Perform a synchronization to one or more hosts, or request that a synchronization be performed on your behalf.
- **Sequence Management:** Create, modify, and delete sequence definitions. Sequences allow the grouping of service operations and synchronization operations to define higher level code deployment operations.
- **Run Sequence:** Perform a pre-defined sequence of service operations and synchronizations on one or more hosts, or request that a sequence be performed on your behalf.
- **View History:** Get information about previously run Code Deployment operations. See “Code Deployment and Rollback” on page 435 in Chapter 12 for more information.

Administration: Expands to display the following features. For more information about these features, see the *Opware® SAS Administration Guide* and *Opware® SAS Policy Setter's Guide*.

- **Users & Groups:** Administrators use this feature to create user groups, define permissions for those groups, create new administrators, and add users to groups.
- **Server Attributes:** Define and edit server use attributes, enable them for code deployment, and define deployment stages. Also define and edit server deployment stage attributes.
- **System Configuration:** Contains the configuration parameters that define how the Opware System works in your environment. This selection is only used at the direction of Opware Inc.
- **System Diagnosis:** Runs a series of tests on Opware components to make sure that they are functioning correctly.
- **Gateway:** Allows you to connect Satellites with this or other cores.
- **Opware Software:** Provides a view of the properties, custom attributes, installation order, and history of the software attached to the Opware SAS in the system.



The Administration set of features is only available if you are logged in as an Opware administrator.

Navigation

Top-level navigation from the Home page is simple. To access any of the features in the navigation panel, click the feature name. To access any of the wizards or other features in the Tasks area of the Home page, click the name of the task.

After you select a task or a feature, other pages appear, which might have one or more of the following means of navigation:

- Clicking a hyperlinked name to display a page
For example, if you select Software ► Scripts (assuming that you have the correct permissions), the page that appears shows all of the scripts that have been uploaded so far.
- Selecting a tab to display a page

For example, when you select Manage Servers and click one of the hyperlinked server names, the resulting page shows a row of tabs, like Figure 2-6 shows.

Figure 2-6: Example of Tabs



Each tab displays a page, each with its own buttons and functionality.

- Clicking a button to display a page

For example, when you select the Custom Attributes tab, a page appears with several buttons: **Add**, **Delete**, and **Copy**, which are common to each page called by these tabs, and **Add Custom Attribute**, which is unique to this particular tab. You will find similar functionality on all tabbed pages in the Opware System.

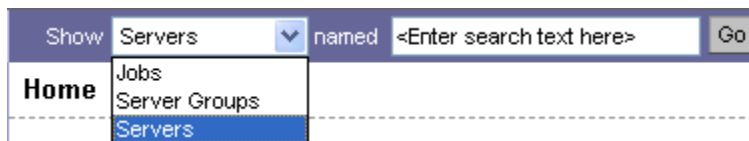
My Profile

You can update your own personal user information without the assistance of the Opware administrator with the My Profile link. You can change your first and last name, your contact information, your password, and your time zone and date display preferences.

Search

At the top of the Home page open the dialog box as Figure 2-7 shows.

Figure 2-7: Search Function



You can search for servers, jobs, and server groups, by making the selection from the drop-down list, and then entering an identifying string in the text box.

My Servers

The My Servers feature provides a convenient place to store a set of servers that have been selected and stored using the Add to My Servers function in Manage Servers. You might use it as a shortcut to the servers you work with most often, or as a way to gather a group of servers when you want to apply the same changes to all of them. All functions that are available in the Manage Servers page are also available from within My Servers.

Mouseover Icon Tooltips

When an icon appears on a page in the SAS Web Client, a tooltip displays information about the icon when your mouse pointer hovers over it. For example, server icons display messages such as “Available or Build Failed” to describe the state of the server. Packages and patches display messages such as Available, Managed, Unmanaged, and so forth.

Chapter 3: Getting Started with SAS Client

IN THIS CHAPTER

This section discusses the following topics:

- Overview of the SAS Client
- Requirements for Running the SAS Client
- Installing and Launching the SAS Client
- SAS Client User Interface
- SAS Client Search
- Accessing SAS Client Options
- Browsing Job Logs

Overview of the SAS Client

The SAS Client is a powerful Java client for the Opware Server Automation System. It provides the look-and-feel of a Microsoft Windows desktop application with the cross-platform flexibility of Java. Over time, more and more of the Opware Server Automation System's features will be available via the SAS Client.

The SAS Client provides the following features:

- Discovery and Agent Deployment
- Server Explorer
- Virtualization Director
- Audit and Remediation
- Visual Application Manager
- Software Management
- Patch Management for Windows
- Patch Management for Unix

- Visual Packager
- Application Configuration Management
- Global Shell
- Integration with NAS

For descriptions of all the SAS Client features, see “Opware SAS Features” on page 40.

Requirements for Running the SAS Client

Java J2SE v 1.4.2_13 JRE must be installed on the system that runs the SAS Client. To download this version of Java, go to <http://java.sun.com/j2se/1.4.2/download.html>. The SAS Client is supported on the following operating systems:

- Windows 2003
- Windows 2000
- Windows XP



When using Internet Explorer, if you try to launch the SAS Client without installing Java J2SE v 1.4.2_13 JRE, you are prompted to install JRE and run the SAS Client in one step. When you select this option, Java v 1.4.2_13 JRE is installed and you get the following error message: `Java Web Start -unexpected Error. Unable to launch SAS Client.` To launch the SAS Client, ignore the error message and click **Retry**.

Installing and Launching the SAS Client

To access the SAS Client for the first time, you must launch the SAS Client installer from the SAS Web Client. You only need to install the SAS Client once.

Once you have downloaded and installed the SAS Client, you can start it from the following locations:

- In the Power Tools section of the SAS Web Client home page
- On your desktop (an SAS Client program icon is installed to your desktop if you choose to install one on your desktop)

- From the **Start** menu, select ► **All Programs** ► **Opware SAS Client**.



By default, the core that you log into is the core of the SAS Web Client where you launched the SAS Client download. You can change the default core by configuring your general options. See “Accessing SAS Client Options” on page 87 in this chapter for more information.

To install and launch the SAS Client, perform the following steps:

- 1** Launch the Opware SAS Web Client and log in.
- 2** From the Home page of the SAS Web Client, in the Power Tools section, click the Launch SAS Client link.
- 3** If you are a Firefox user, open the JSP file to launch the SAS Client installation. (Internet Explorer users should go to the next step.)
- 4** After the SAS Client has been downloaded to your computer, the Login window displays, as seen in Figure 3-1. Enter your user name and password, and click **Login**.

Figure 3-1: Login the SAS Client Window.

The screenshot shows a login window titled "Please login...". The window has a blue header bar with standard window controls (minimize, maximize, close). The main content area is white and features the Opware logo, which consists of the word "OPWARE" in a bold, sans-serif font with a blue swoosh underneath, and the words "SERVER AUTOMATION" in a smaller, blue, sans-serif font below it. Below the logo, there are three input fields. The first is labeled "User Name:" and is empty. The second is labeled "Password:" and is empty. The third is labeled "Core Server:" and contains the text "occ.c03.dev.opware.com". At the bottom of the window, there are two buttons: "Login" and "Cancel".

The user name is not case sensitive. If you have access to more than one core server, you can enter the core server's IP address or name in the core server field. If you don't specify a port with the host:port notation, port 443 is used.

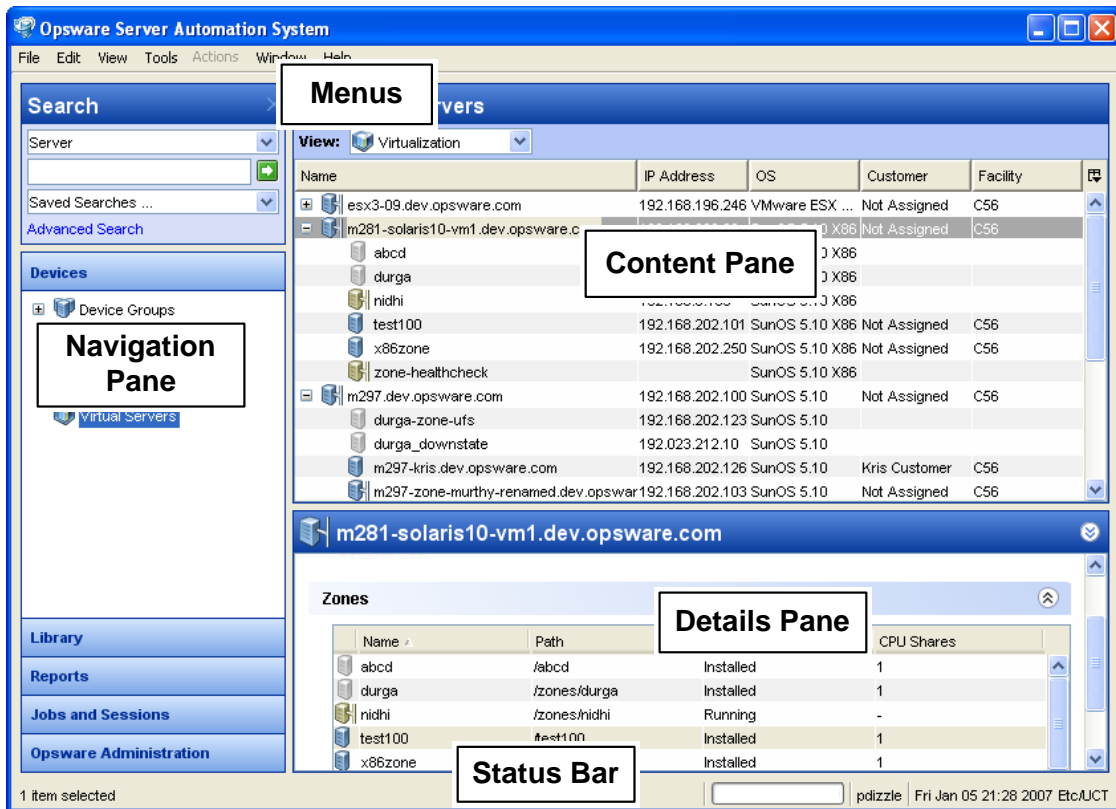
- 5** If you are asked to accept the certificate from the core server, click **Yes**. The SAS Client now appears.

SAS Client User Interface

The SAS Client user interface provides easy access to all of the SAS Client features and functionality. The SAS Client user interface has six main areas:

- Menu
- Navigation Pane
- Search
- Content Pane
- Details Pane
- Status Bar

Figure 3-2: SAS Client User Interface



Menus

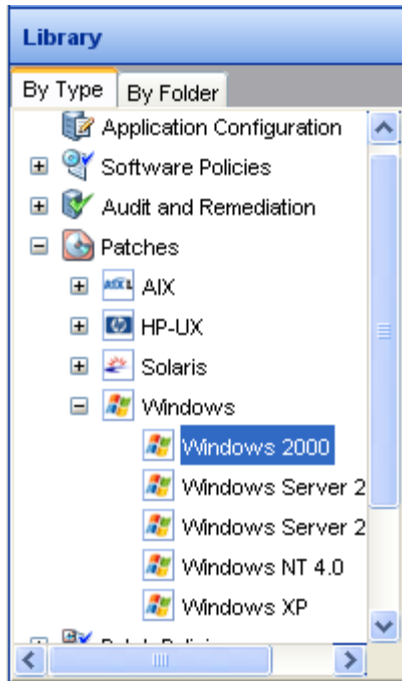
The SAS Client includes the following menus:

- **File:** This enables you to open a new SAS Client window, or close the current window, or exit all open SAS Client windows.
- **Edit:** This enables you to cut, copy, paste, and delete text.
- **View:** This refreshes the current view and shows the latest information from the core that you are currently logged into (such as compliance test information for the compliance dashboard). You can also access SAS Client features in the Navigation pane, such as Devices (groups of devices, managed and unmanaged servers), Reports (Compliance Dashboard, Reports) Software Library (application configuration, server compliance, patch management), OS sequences and OS installation profiles, Jobs and Sessions (job logs and shell sessions), and Opsware Administration (patch settings and patch compliance rules). This also allows you to show or hide the Action pane and the Preview pane.
- **Tools:** This enables you to open a Global Shell session, open the Visual Application Manager, or access the SAS Client options.
- **Actions:** Depending upon the feature that you have selected in the Navigation pane, this menu enables you to perform numerous functions related to all main SAS Client features.
- **Window:** This enables you to access multiple instances of SAS Client windows, if more than one window is open.
- **Help:** This menu provides help for the SAS Client. Help F1 provides context-sensitive help relevant to the current feature window selected or opened (same as F1). The contents and index will open the SAS Client help system to the main table of contents. (The About SAS Client menu provides version and system information.)

Navigation Pane

To access SAS Client features, select a feature in the Navigation pane, as shown in Figure 3-3. When you select a feature, the contents of it appear in the Content pane. You can access functions related to it through the Actions menu.

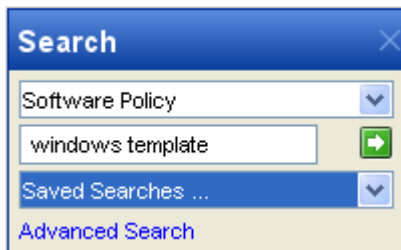
Figure 3-3: Navigation Pane



Search

The Search feature allows you to search for any information in Opware SAS, such as SAS Client Server, Device Group, Folder, Job, Software, Patch, Application Configuration, Software Policy, Patch Policy, Audit, and Snapshot Results. For more information on how to use the search tool, see “SAS Client Search” on page 82.

Figure 3-4: Search in the SAS Client



Content Pane

Depending on the selection in the Navigation pane (Devices, Library, Reports, Jobs and Sessions, Opsware Administration), the Content pane lists the following information:

- All managed servers and device groups, including unmanaged servers – both physical and virtual
- Agent deployment information
- Application Configurations and Application Configuration Templates
- Software Policies
- Audit and Remediation audits, audit policies, and snapshots
- Patches and patch policies
- OS installation profiles and OS sequences
- Packages
- Reports and the Compliance Dashboard
- Custom attributes
- Jobs that the user has run
- Access to the Global Shell sessions
- Patch configuration and patch compliance rules

Figure 3-5 is an example of the Content pane for managed servers. You can perform actions on features in the Content area using the Action Menu or Action Pane, or you can right-click to perform various actions or double-click to open.

Figure 3-5: Feature Content Window Showing the Managed Server

The screenshot displays the 'All Managed Servers' window. At the top, there is a 'View:' dropdown set to 'Properties' and a search box for 'Name'. Below this is a table listing several servers. The server 'm080.dev.opsware.com' is selected and highlighted in blue. Below the table, a detailed view for this server is shown, titled 'm080.dev.opsware.com'. This view includes 'Management Information' with the following details:

- Name: m080.dev.opsware.com
- Notes:
- IP Address: 192.168.165.156
- OS Version: SunOS 5.9
- Customer: Not Assigned
- Facility: C44
- Realm (link speed): Transitional

Name	IP Address	OS	Customer
bantry.snv1.corp.opsware.com	192.168.8.154	Windows 2003	Not Assigned
C - 720044	192.168.8.136	Windows 2003	Not Assigned
dgokina.localdomain	192.168.8.114	Red Hat Ente...	Opsware
glengarriff.opsware.com	192.168.8.142	Windows 2000	Not Assigned
hfarhi_txp2.opsware.com	192.168.8.73	UNKNOWN	Not Assigned
m022.qa.opsware.com	192.168.160....	Red Hat Ente...	Arnold
m080.dev.opsware.com	192.168.165....	SunOS 5.9	Not Assigned
m103.qa.opsware.com	192.168.160....	SunOS 5.10	Arnold
m120	192.168.160....	Windows 2003	Arnold
m157.qa.opsware.com	192.168.160....	AIX 5.3	Arnold

Content Pane Tools

From inside the Content pane, you can perform the following actions:

- With the View drop-down list, you can change the view of a selected feature. For example, you can select a server from the Content pane, and then from the View drop-down list, choose Installed Packages. This shows all packages installed on the server, as shown in Figure 3-6.

Figure 3-6: View Drop-down List



- In the column headings of the Content pane, you can sort data about a feature. For example, for a managed server, you can sort by Server Patch Compliance, IP address, OS, and so on.
- With the search tool, you can search the Content pane by feature or by attribute, as shown in Figure 3-7.

Figure 3-7: Search Tool



Details Pane

The Details pane allows you to preview information about servers, device groups, patches, and patch policies selected in the Content pane without having to open a new window.

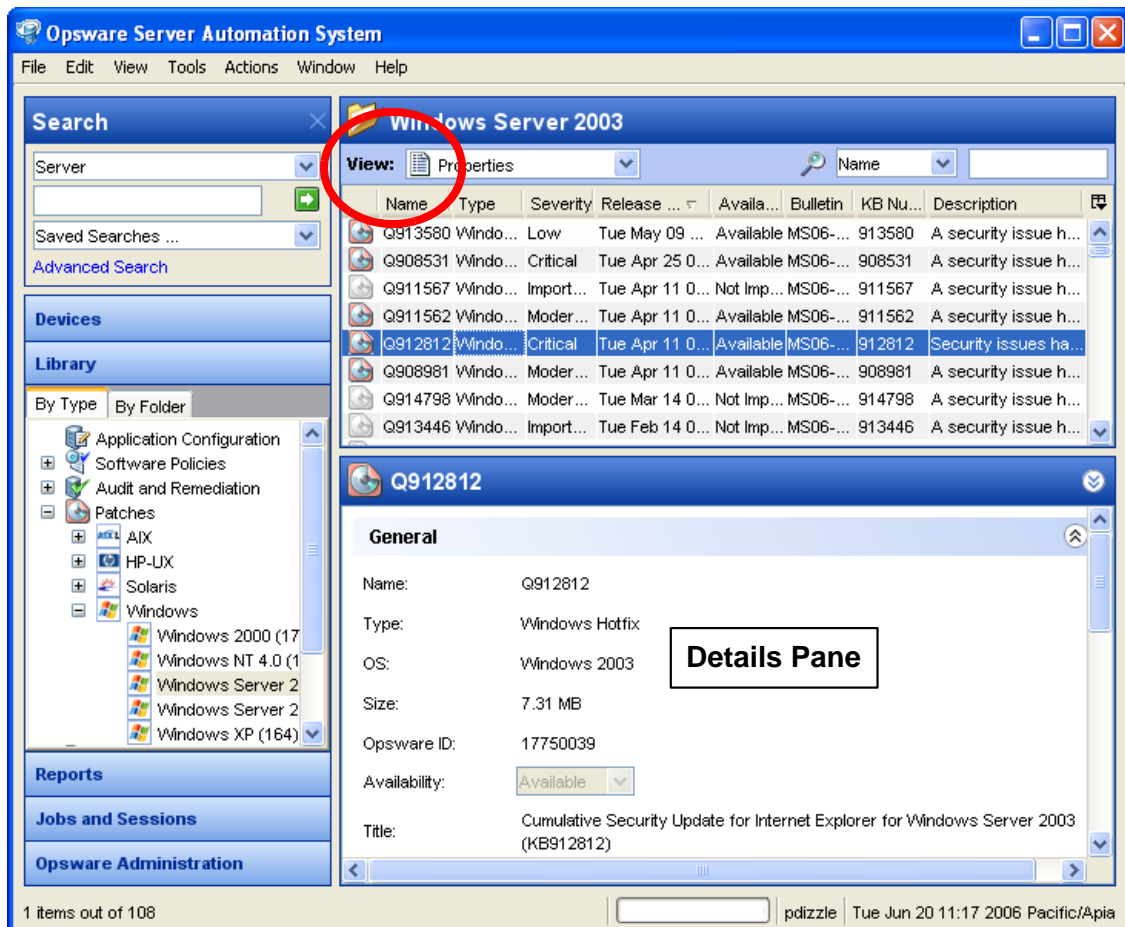
You can use the Details pane to perform the following actions:

- Preview information about a server, device group, patch, or patch policy. To do so, select it in the Content pane.

- Filter the type of information you view in the Details pane. From the top of the content area, choose a view from the View drop-down list.
- Deactivate the Details pane. To do so, from the **View** menu, select **Details Pane ► Minimize**.

For example, if you are viewing Windows 2003 patches from the Library, you can select a patch in the Content pane and see information about the patch in the Details pane. This is shown in Figure 3-8.

Figure 3-8: Main Application Windows Showing Patch Properties Information in the Preview Pane



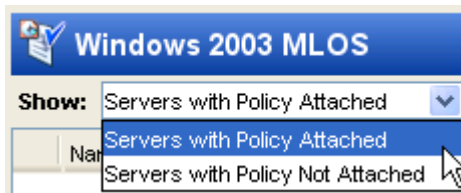
To view other types of information about the selected patch, from the View drop-down list, choose a view.

Details Pane Show Filter

Some features displayed in the Details pane allow you to further filter the feature. Using the Show drop-down list, you can choose different views of the feature.

For example, if you are viewing all of the servers that the patch policy is attached to, in the Details pane, you can filter either Servers with Policies Attached or Servers with Policies Not Attached, as shown in Figure 3-9.

Figure 3-9: Details Pane Show Drop-down List



Status Bar

At the bottom of the SAS Client Application window, the status bar provides the following information:

- Informational text (left hand side) about the selected object
- A progress bar that shows progress on retrieving information from the core
- The user ID
- The current Opsware SAS time

Figure 3-10: SAS Client Status Bar



SAS Client Search

In the SAS Client, you can search for any information about your operational environment that is available in Opsware SAS using the SAS Client Search feature. The Search feature enables you to search for Application Configuration, Application Configuration Template, Audit, Device Group, Folder, Job, Patch, Patch Policy, Server, Snapshot Result, Software, and Software Policy.

The SAS Client Search feature enables you to perform the following actions:

- Perform a simple search by using keywords.

- Perform an advanced search by creating search queries.
- Save a search query.
- Perform actions on search results.
- Email search results.
- Print search results.
- Customize search results formatting.



You cannot search for Custom Fields on servers using the SAS Client Search feature. To search for Custom Fields on servers, use Server Search in the SAS Web Client. See “Server Search” in *Opware® SAS User’s Guide: Server Automation* for more information.

Performing a Simple Search

In the SAS Client, a simple search enables you to search for items by entering a keyword in the search text field. When you enter a keyword or text, simple search carries out a “contains” operator search on the entered text.

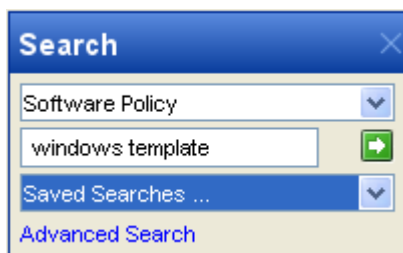



The search operation returns only items on which you have at least read permissions. To perform an action on an item, you must have write permission on that item.

To carry out a simple search, perform the following steps:

- 1** From the Navigation pane, select Search.
- 2** To display Search in the Navigation pane, select **Search Pane** from the **View** menu.
- 3** From the drop-down list, select the item you want to search as shown in Figure 3-11.

Figure 3-11: Simple Search in the SAS Client



- 4** Enter the search text in the text field. The SAS Client search feature does not support a wildcard search and the search is not case sensitive.
- 5** Click  to search. The search results appear in the Content pane.
- 6** (Optional) Click on any column heading to sort the search results. You can also change the order of the columns by dragging the column heading and dropping it into the desired location.
- 7** (Optional) Click **Save** to save your search query. The Save Search window appears. Enter the name of the search and click **Save**. The name of the saved search cannot be more than 64 characters. See “Creating a Device Group Groups Using Search” on page 167 in Chapter 5 for information about saving a search query as a device group.
- 8** (Optional) Click **Export** to export search results. The Export Results window appears. Enter the location, the file name and the file type and then click **Export Results**.
- 9** (Optional) After you export the search results, you can email the search results by attaching the exported file to the email. You can also print the search results by printing the exported file from an application that supports .csv or .html files.
- 10** (Optional) To perform an action on the search results, select an item from the Content pane and then from the **Actions** menu, select the appropriate action.

Performing an Advanced Search

In the SAS Client, an Advanced search enables you to create complex queries on search items. In a search query, you can specify up to five rules and combine each rule with a logical “And” or “Or” operator. You cannot use both the “And” and “Or” operator in a single search query. Each rule is a combination of an attribute/operator/value that enables you to search for a specific attribute value for the selected search item. Depending on the attribute that you select, the options for the operator and value are displayed. You can specify the attribute values by entering text or a numerical value in the text field, by selecting a value from the drop-down list, or by selecting multiple values from a list of values in the Select Values window.

The Select Values window appears when you need to specify multiple values for a rule containing an “equals” or “not equals” operator. In this window, you can select multiple values from the list or add values to the Available field.



The search operation returns only items on which you have at least read permissions. To perform an action on an item, you must have write permission on that item.

To carry out an advanced search, perform the following steps:

- 1** From the Navigation pane, select Search. To display Search in the Navigation pane, select the **Search Pane** from the **View** menu.
- 2** Click **Advanced Search**. The Advanced Search page appears in the Content pane. By default, the search item Server is selected in the first drop-down list and one search rule is added to the search.
- 3** From the first drop-down list, select the item you want to search.

Figure 3-12: SAS Client Search

The screenshot shows the SAS Client Search interface. On the left is a navigation pane with 'Search' selected. The main area is titled 'Advanced Search' and contains several configuration fields:

- Search Item: Software Policy
- Attribute: Created By
- Operator: Contains
- Value: alfred
- Logic: And (selected)
- Additional rules: Lifecycle (Equals, Available) and Created Date (Before, Fri 06/16/2006)

Below the configuration is a table of search results:

Name	Location	Created By	Created Date	Lifecycle
Demo Policy for Conference ...	/alfred	alfred	Sun May 28 05:00:53 2006	AVAILABLE
Policy for AIX	/alfred	alfred	Sat May 27 01:37:20 2006	AVAILABLE
Policy for RH AS3	/alfred	alfred	Tue May 23 07:15:00 2006	AVAILABLE
Policy for Win2k	/alfred	alfred	Thu May 25 06:23:12 2006	AVAILABLE
Policy to Verify Bugs	/alfred	alfred	Thu May 25 21:10:38 2006	AVAILABLE
Windows Template	/2/New Folder (6)	alfred	Sat May 27 01:42:05 2006	AVAILABLE

- 4** Create a rule by selecting the attribute from the second drop-down list. Depending on the attribute that you select, options available for the operator and values for the rule will change.
- 5** Select the operator from the third drop-down list. The operator selected defines how the search text is treated.
- 6** Enter a value in the field or select a value from the drop-down list or click to select multiple values from the **Select Values** window.
- 7** Click to add additional rules and repeat steps 4 to 6. Click to delete any rules.
- 8** Select the logic (And/Or) to be applied for every rule in the query.

- 9** Click **Search** to run the search query. The search results appear in the Content pane.
- 10** (Optional) Click **Reset** to clear the search query rules or click **Cancel** to cancel the search operation.
- 11** (Optional) Click on any column heading to sort the search results. You can also change the order of the columns by dragging the column heading and dropping it into the desired location.
- 12** (Optional) Click **Save** to save your search query. The Save Search window appears. Enter the name of the search query and click **Save**. The name of the saved search cannot be more than 64 characters. The saved search query appears in the Saved Searches. See "Creating a Device Group Groups Using Search" on page 167 in Chapter 5 for information about saving a search query as a device group.
- 13** (Optional) Click **Export** to export search results. The Export Results window appears. Enter the location, file name and file type (.csv or .html) and then click **Export Results**.
- 14** (Optional) After you export the search results, email the search results by attaching the exported file to the email. Or, print the search results by printing the exported file from an application that supports .csv or .html.
- 15** (Optional) To perform an action on the search results, select an item from the Content pane and then from the **Actions** menu, select the appropriate action.

Running a Saved Search Query

To run a saved search query, perform the following steps:

- 1** From the Navigation pane, select Search.
- 2** From the Saved Searches drop-down list, select a search query. The query appears in the Content pane.
- 3** Click **Search** to run the query. The search results will appear in the Content pane.

Deleting a Saved Search

To delete a saved search query, perform the following steps:

- 1** From the Navigation pane, select Search.
- 2** From the Saved Searches drop-down list, select a saved search query. The saved search appears in the Content pane.

- 3 Click **Save**. The Saved Search window appears.
- 4 Select the saved search and click **Delete**. Click **Delete** on the Confirmation window to delete a saved search.

Accessing SAS Client Options

You can configure the following options for the SAS Client:

- **General Options:** This enables you to set options such as choosing the core you want to log into by default, how to handle caching, and so on.
- **Unmanaged Servers:** This enables you to set options for the Opsware Agent Discovery and Deployment (ODAD) feature.
- **Packaging Servers:** This enables you to view and specify packaging servers available on the core.
- **Terminal and Shell:** This enables you to configure your Terminal (UNIX) and RDP (Windows) client for the Global Shell and Remote Terminal connections.
- **Patch Policies:** This enables you to specify that a confirmation message will display when you try to remove a patch policy or a patch policy exception from a managed server.
- **Visual Application Manager (VAM) Options:** This enable you to specify timeout values for launching VAM and the manner in which you want VAM to scan virtual server relationships.
- **Opsware NAS:** This enables you to reset the name of the NAS host that you log into, restore the previously saved (default) host name, and launch the NAS login window.

Accessing SAS Client Options

To set SAS Client options, perform the following steps:

- 1 From the **Tools** menu, select **Options**.
- 2 From the left side of the Set Options window, choose an option.

General Options

The following general options enable you to select your default core:

Core Server Defaults

This option allows you to configure the core that you log into from the SAS Client. Options include:

- **Host:** This enables you to choose the name or IP address of the SAS Web Client host that you log into by default.
- **Port:** This enables you to choose the port number of the SAS Web Client host that you log into by default; 443 is the default.

Cache

This option enables you to configure the caching of data displayed inside the SAS Client. You can configure the following cache settings:

- **Check for updates every X minute(s):** This enables you to enter a value for how many minutes will pass before the cache is refreshed.
- **Update Cache:** This enables you to check instantly for new information from the core.
- **Reload the Cache:** This enables you to immediately reload (refresh) the cache.

Progress Information

This option shows the progress of a job. When a job finishes, the Progress window closes.

Equals Operator Limit in Search and Reports

This sets limits on the number of available value selections in the Advanced Search and Reports interfaces. To prevent delays and excessive system load, the list of available values is not populated when the number of values exceeds this setting. Values are added by entering them in a text box.

Unmanaged Servers

These options allow you to control the operation of the ODAD. You can set the following ODAD options:

- Installer Options
- Protocols
- Advanced

See Chapter 4, "Opware Agent Management" on page 99 of this guide for more information.

Installer Options

From the Installer Options window, you can set the Installer options and control the installation of an Opware Agent on a server. The Installer Options window enables you to perform the following actions:

- **Start the Opware Agent after Installation:** This enables you to start the Opware Agent after installing it on the server. By default, the Opware Agent Installer does not start the Opware Agent.
- **Remove existing machine IDs and cryptographic material:** This enables you to remove any existing machine specific identifying materials, such as the Machine ID file (MID), and all machine-specific cryptographic material from the server.
- **Ignore prerequisite check failures:** This enables you to ignore prerequisite check failures and forces Opware Agent installation.
- **Set the server's time from the Opware core:** This enables you to synchronize the time on the server in which the Opware Agent is installed with the Opware core.
- **Install Windows Installer (MSI) if required:** This enables you to install MSI along with the Opware Agent. If MSI is already installed, this option has no effect.
- **Install Windows Management Instrumentation (WMI) if required:** This enables you to install WMI along with the Opware Agent. If the WMI is already installed, this option has no effect.
- **Reboot Windows servers after agent installation:** This enables you to reboot Windows servers after the Opware Agent installation is complete.
- **Install Red Hat Package Manager (RPM) on AIX and Solaris:** This enables you to install the RPM handler with the Opware Agent. Opware recommends that you always include this option when you install Opware Agents on Solaris and AIX servers.
- **Reset Opware Agent configuration, if present:** This enables you to replace the existing Opware Agent configuration.
- **Delete gateway address list, if present:** This enables you to delete the Opware Gateway address list, if present and no longer required.
- **Overwrite staged Opware Agent installer:** This enables you to overwrite the existing Opware Agent Installer.
- **Log Level:** This enables you to set the log level for log messages. With this option, you can specify levels for error, warning, info, and trace.

Protocols

The Protocol window allows you to specify the standard port to connect to the servers for deployment. The following protocols are used:

- **SSH:** This enables you to determine the standard port to connect to the servers for deployment using the SSH protocol.
- **Rlogin:** This enables you to determine the standard port to connect to the servers for deployment using the Rlogin protocol.
- **Telnet:** This enables you to determine the standard port to connect to the servers for deployment using the Telnet protocol.
- **NetBIOS:** This enables you to determine the standard port to connect to the servers for deployment using the NetBios protocol.
- **WTS:** This enables you to determine the standard port to connect to the servers for deployment using the WTS protocol.

Advanced

The Advanced Installer Options window allows you to set the following options:

- **Immediately do a full hardware registration:** This enables you to force the Opware Agent Installer to report full hardware information to the core.
- **Immediately do software registration:** This enables you to force the Opware Agent Installer to report full software information to the core.
- **Suppress Opware Agent reachability check:** This enables you to disable this check during installation. By default, the installer triggers the core to check if the server is reachable.
- **Disallow anonymous SSL connections if Opware Agent is dormant:** This enables you to configure the Opware Agent so that browsers cannot connect without a valid certificate.
- **Force creation of new device record if conflict found:** This enables you to suppress this functionality. During registration, the Data Access Engine creates a new device record.
- **Fail if initial hardware registration fails (do not go dormant):** This enables you to ensure that the Opware Agent does not become dormant, if it fails to report hardware information.

- **Do not open Windows Firewall for core-agent communications:** By default, the Opsware Agent Installer will modify the Windows Firewall configuration on Windows XP and Windows 2003 (r2) servers to allow the Opsware core to contact the managed server on port 1002. If you select this option, the firewall configuration will not be modified. The server may not be manageable by Opsware in this case.
- **Remediate software policies:** This enables you to remediate the server against any software policies attached to the server.
- **Attach to software Policy ID:** This enables you to attach the server to the software policy ID.
- **Reconcile Type:** This enables you to reconcile the server against any nodes assigned to the server. The reconcile type can be Full or Add only.
- **Attach to template ID:** This enables you to assign the nodes contained in the template to the server.
- **Install directory (UNIX):** This enables you to specify the directory where the Opsware Agent will be installed. By default, the Agent is installed in `/opt/opsware/agent` on UNIX, and `%ProgramFiles%\Opsware\agent` on Windows.
- **Extra Installer options:** This enables you to specify any other installer options.
- **nmap parameters:** This option allows you to specify parameters used when scanning for unmanaged servers. If you find that the Opsware Discovery and Agent Deployment is unable to correctly locate and identify unmanaged servers due to the network firewall configuration, you can specify a different set of scan parameters. See the nmap documentation for more information.

Packaging Servers

To create packages with the SAS Client, you need to configure a managed server in your Opsware core as a packaging server.

The Set Options window lists all configured packaging servers on the core. To sort the list alphabetically by operating system, click the OS column heading. To sort this list of servers by existing configured packaging servers, click the Default Server column heading. For servers that are already configured as packaging servers, the IP address is displayed in this column. For servers that are not configured as packaging servers, Not Configured is displayed in this column.

To configure a packaging server, perform the following steps:

- 1** In the right pane, select a managed server and click **Edit**.
- 2** In the Select Server window, select the managed server that you want to configure as the packaging server and then click **Select**. In the Set Options window, the Default Server column will now display the IP address of the server. (Before you configured this as the packaging server, the Default Server column displayed Not Configured.)
- 3** In the Set Options window, click **Save** to save your changes or click **Cancel** to close this window without saving your changes.

Terminal and Shell

These settings define the command that the SAS Client invokes on your PC to open a Global Shell or Remote Terminal session. (For instructions on using an `ssh` client instead of the SAS Client, see "Opening a Global Shell Session" on page 386.)

Terminal Client

This setting specifies the terminal client that the SAS Client uses for Remote Terminal sessions on Unix managed servers and for Global Shell sessions. The default value is:

```
cmd /c start /w cmd /c "telnet %h %p && echo %m && pause > nul"
```

The `telnet` program emulates a command-line terminal session. The `%h` represents the host and the `%p` is for the port. (See Table 3-1.)

If you change the Terminal Client setting from the default value, make sure that the command blocks until the terminal application terminates. The terminal application must not run in the background. If you specify `cmd /c start`, include the `/w` switch to make `cmd` block until the underlying command (such as `telnet`) completes.

You are not required to use `telnet` as the terminal application. For example, to use a PuTTY client, specify the following command:

```
"C:\\Program Files\\putty\\putty.exe" -telnet %h %p
```

RDP Client

This setting specifies the Remote Desktop Protocol (RDP) client that the SAS Client uses for Remote Terminal sessions on Windows managed servers. The default value is the Microsoft Terminal Services Client:

```
mstsc "%r"
```



The SAS Client supports the Windows XP version of the Remote Desktop Connection Software, which can be downloaded from the following URL:

<http://www.microsoft.com/windowsxp/downloads/tools/rdclientdl.mspx>

The specified terminal client must be installed on your PC. To verify the existence of the terminal client, click **Test**.

The command can include variables such as %h and %p. When the terminal client is launched, these variables are replaced with the values shown in Table 3-1. To override a replacement value, specify a constant instead of a variable. For example, you might specify 435 for the port instead of %p.

Table 3-1: Variables for the Terminal and RDP Client Options

VARIABLE	DESCRIPTION	REPLACEMENT VALUE
%e	The character encoding.	For Remote Terminal sessions, the encoding of the managed server. For Global Shell sessions, the value of the Encoding field.
%h	The host name that the telnet client connects to.	The value of the localhost of the managed server.
%m	A locale-specific message on how to close the window.	For English locales, click the Enter key to close this window.
%p	The port that the telnet client connects to.	A randomly chosen port.
%r	The name of the Remote Desktop (RDP) connection file. This variable is used only for the Microsoft Terminal Services Client (mstsc).	A temporary RDP file generated at runtime by the SAS Client.
%t	The title displayed in the terminal window.	For Remote Terminal sessions, the name of the managed server. For Global Shell sessions, the string "Global Shell."

Encoding

This setting sets the encoding for Global Shell and the Remote Terminal sessions. This option is the replacement value of the %e variable in the command specified by the Terminal Client field. The default value of the Encoding option is UTF-8.

Patch Policies

This option allows you to specify that a confirmation message will display when you try to remove a patch policy or a patch policy exception from a managed server.

Visual Application Manager (VAM) Options

For VAM, you can specify the following options:

- Virtualization Settings
- Scan Time-Out Preference

Virtualization Settings

You can configure SAS Client options that allow you to choose whether or not you want to perform a scan on any virtual servers or hypervisors related to the virtual server you want to open in VAM.

For example, if you want to visualize a VMware virtual machine (VM) or Solaris local zone in VAM, by default you will be asked if you also want to scan any virtualization relationships – in other words, the system asks if you want VAM to also scan the hypervisor that is hosting the selected virtual server. Depending upon the virtual server you select, VAM might have to scan several related virtual servers in order to visualize a single virtual server in VAM.

Conversely, if you select a hypervisor to open in VAM, you will also be asked if you want to scan any virtualization relationships – in this case, VAM would need to scan all of the hosted virtual servers, which could take a long time to perform.

By default, VAM will always ask you if you want to scan virtual relationships, but you can set your own default behavior for scanning related virtual servers with the following virtualization options:

- Ask each time if you want to scan related virtual and host servers.
- Always scan related virtual and host servers.
- Never scan related virtual and hypervisor servers.

To change the virtualization settings, perform the following steps:

- 1** From the **Edit** menu, select **Options**.
- 2** In the Set Options window, in the Views pane, select Visual Application Manager.
- 3** Specify your desired Virtualization Settings, then click **OK** when you are finished.

Scan Time-Out Preference

VAM is optimized to scan a maximum of 50 servers. A number of factors affect the time it takes for a scan to complete, including the load on the scanned servers and the load on Opsware. The default scan time-out is set to 300 seconds. You can reset this time-out value to a minimum of 30 seconds or to a maximum of 3600 seconds.

To change the scan time-out, perform the following steps:

- 1** From the **Edit** menu, select **Options**.
- 2** In the Set Options window, in the Views pane, select Visual Application Manager.
- 3** In the Scan Timeout section, move the slider to increase or decrease the number of seconds at which you want the scanning process to stop.
- 4** Click **OK** to save your changes or click **Cancel** to close the window without saving your changes.

Opsware NAS

This options allows you to reset the name of the NAS host that you log into, restore the previously saved (default) NAS host name, and test whether SAS can communicate with NAS by using the new host name.

- **Host:** This option specifies the name of a server that is acting as a proxy for the NAS host. Only the format of the host name is verified.
- **Restore Default:** This option restores the previously saved NAS host name.
- **Test:** This option opens the Opsware NAS login window to verify whether the host name is valid.

Browsing Job Logs

A job is any major process run by the Opsware SAS Web Client or the SAS Client, such as a communication test, a software installation, an OS installation, audit results remediation, an Application Configuration push, a server compliance audit, and so on.

The Job Logs window shows the details of all jobs run under the currently logged in user name and jobs that are currently in progress. It also displays jobs scheduled to run, including the name of the job, the start time, the number of servers affected by the job, and the status of the job.

The display of a job's start time and finish time is determined by original user preferences set in the SAS Web Client, which may be different than those of the current user. If a user is working in multiple times zones, it is a good idea to make sure that these preferences are set to display the time zone in the date.

To see the details of a finished job, open a job. If the job is recurring (scheduled to be run), then opening the job will cause the Schedule Job window to display. You will only be able to modify the scheduled job if you created the job, or have Edit All Jobs permissions. To obtain these permissions, contact your Opsware administrator. See the *Opsware® SAS Configuration Guide* for more information.

You can search the job list by selecting the following criteria (located at the top of the Job Logs window):

- **Job ID:** This enables you to enter the job ID.
- **Job Type:** This enables you to choose a type of job from this list.
- **Time Restrictions:** This enables you to limit the search for a job by a time restriction such as the last week, last two weeks, or last month.
- **Ticket ID:** This enables you to enter a ticket ID here if one was given for the job.
- **Job Status:** This enables you to choose a job status, such as job completed, completed with errors, cancelled, and so on.
- **User name:** This enables you to enter your user name to see only those jobs you have run, or enter nothing here to show all jobs. Click on the column header to sort the list. Only users with the View All Jobs or Edit All Jobs permissions will be able to view all jobs in the core. If you do not have these permissions, you will not be able to see all jobs.

To view a job, select it, right-click, and select **Open**.

To stop a job that is currently running, select it, right-click, and select **Stop**.

Recurring Schedules

The recurring schedules window shows all jobs that are scheduled to run on a recurring basis. You can choose to view all recurring jobs, or filter the list of recurring jobs by the following methods:

- **Any ID:** This enables you to enter the job ID.
- **Any Type:** This enables you to choose a type of job from this list.
- **Any Ticket:** This enables you to enter a ticket ID here if one was given for the job.
- **Any User:** This enables you to enter your user name to see only those jobs you have scheduled to run on a recurring basis, or enter nothing here to show all recurring jobs. Click on the column header to sort the list. Only users with View All Jobs or Edit All Jobs permissions will be able to view all jobs in the core. If you do not have these permissions, you will not be able to see all jobs.

To view a recurring job schedule, select it, right-click, and select **Open**.

To delete a recurring job, select it, right-click, and select **Stop**.

Chapter 4: Opsware Agent Management

IN THIS CHAPTER

This section discusses the following topics:

- Opsware Agent on Managed Servers
- Opsware Discovery and Agent Deployment
- Opsware Agent Installation Using ODAD
- Viewing Unmanaged Server Information
- Agent Reachability Communication Tests

Opsware Agent on Managed Servers

This section provides information about the Opsware Agent on managed servers and contains the following topics:

- Overview of the Opsware Agent on Managed Servers
- Security for Opsware Agents Running on Managed Servers
- Opsware Agent Functionality on Managed Servers
- Server Information that the Opsware Agent Tracks

Overview of the Opsware Agent on Managed Servers

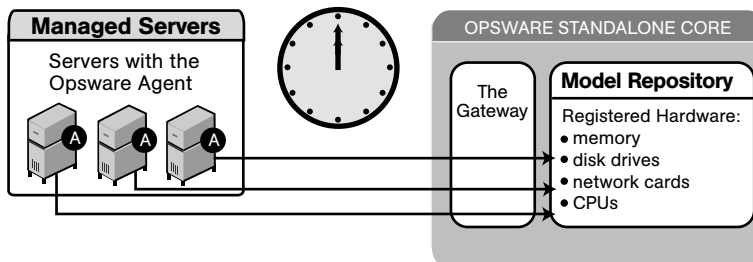
The Opsware Agent regularly performs management tasks on each server autonomously:

On a regular interval, the Opsware Agent gathers a hardware and software inventory of each managed server. It opens a secure communication channel to the Opsware core, presenting its IP address and public-key certificate for authentication purposes. If properly authenticated, the Opsware Agent is permitted to write its updates about the server to the Opsware Model Repository.

Every 12 hours, the Opsware Agent submits hardware information for the managed server on which it is running. Hardware registration also occurs during Opsware Agent installation or software installation. Every 24 hours, the Opsware Agent submits software information for the managed server to the Opsware core. See Figure 4-1.

Figure 4-1: Server Management Tasks Performed by Opsware Agent

Every 12 hours the Opsware Agent inventories the managed servers it runs on, registering hardware information in the Opsware System Core.



The Reporting field indicates the status of the Opsware Agent's reporting capability and tells you whether or not the Opsware Agent is reporting regularly and successfully. The four possible reporting states for the Opsware Agent are as follows:

- **OK:** The Opsware Agent is reporting properly.
- **Registration in progress:** The Opsware Agent is currently registering server hardware information.
- **Reporting error:** The Opsware Agent encountered an error while trying to report hardware information.
- **Last reported days ago:** This indicates when the Opsware Agent last reported.

You can access Opsware Agent reporting information in Server Properties by using advanced search, and by viewing managed servers by Communication status. When viewing by Communication status, the SAS Web Client user interface displays this information in the registration column.

If the Opsware Agent experiences an error in reporting, or has not reported within 24 hours, you can run a Communication Test to troubleshoot the problem.

If you modify the server hardware, it could take up to 12 hours for the change to appear in the SAS Web Client user interface, depending on the time that the Opsware Agent for that server contacted the Opsware core.

If you install or uninstall software on a managed server outside of Opsware SAS, it could take up to 24 hours for the change to appear in the SAS Web Client user interface. For example, if you update the Microsoft Patch Database, it could take up to 24 hours for all managed servers to display whether they need new patches based on the updated Microsoft Patch Database.

In some cases, not all of a server's hardware information is reported. For example, if the Opsware Agent was installed with its default settings, not all hardware information is reported to the SAS Web Client until an hour after the agent is installed. There also might be a problem retrieving certain hardware information, such as a disk failure, that could prevent some hardware information from being reported. In these cases, the server's property page lists unreported information as not set.

If configuration tracking is enabled for a server, the Opsware Agent sweeps through the managed server on a regular interval to see if any of the configurations being tracked are changed. If a tracked configuration is changed, the Opsware Agent performs the action specified by the tracking policy, namely, writing the information to a log file, generating a backup, or sending an email message through SMTP to the email address specified in the tracking policy.

Security for Opsware Agents Running on Managed Servers

Opsware Agents act as both clients and servers when they communicate with Opsware SAS. All communication is encrypted, integrity-checked, and authenticated using X.509v3 client certificates using SSL/TLS.

A small number of Opsware core components can issue commands to the Opsware Agent over a well-defined TCP/IP port. The Opsware Agent can also call back to Opsware core components, each with its own well-defined port.

The Code Deployment & Rollback (CDR) feature uses agent-to-agent communication for performance reasons. In particular, CDR synchronizations (the process of copying changed files and directories from one server to another) happen when an Opsware Agent connects to another Opsware Agent and sends across the network files that have changed since the last time the two Opsware Agents connected.

To further safeguard the SSL/TLS-based communication channel, the two Opsware Agents participating in the code deployment also need to have a common shared secret provided by the Command Engine. Before one Opsware Agent can begin a file transfer to

another Opsware Agent, the two agents must verify that they have a common shared secret provided on a per-session basis by the Command Engine. This safeguard prevents unauthorized users from copying files from one managed server to another.

Opsware Agent Functionality on Managed Servers

The Opsware Agent is designed such that:

- It can only discover information about its own managed server (and no others).
- It cannot make changes on a server unless explicitly instructed to do so by an Opsware core component.

Opsware SAS runs with administrator privileges (root on UNIX servers and Local System on Windows servers), because it performs tasks that require administrator privileges, such as installing patches and rebooting servers.

The Opsware core performs client authentication and, checks to see if the presenting certificate belongs to that particular server. Opsware SAS does this by comparing the certificate to the server's IP address that is generated when the Opsware Agent is initially installed. If the certificate is not valid or the originating IP address does not match the IP address stored in the Opsware Model Repository, authentication fails and the Opsware Agent cannot continue communication with Opsware SAS.

If an unauthorized user were able to log on to a managed server with administrator privileges and compromise a server's security, the user would have only limited access to the following information in the Opsware Model Repository:

- The server's own hardware inventory (already available to someone logged on with administrator privileges)
- The server's own software inventory (already available to someone logged on with administrator privileges)
- The custom attribute information

Server Information that the Opsware Agent Tracks

For each managed server, the Opsware Agent reports software, networking, and hardware information, as shown in Figure 4-2 and Figure 4-3. By communicating with the Opsware core and reporting the installed hardware and software for the server, Opsware SAS determines what software should be installed on a server.

Figure 4-2: Manager Servers: Properties Page-Server Information

Manage Servers: Properties | core.tr3.opsware.com

[Return to Manage Servers](#)

Properties	Network	Membership	Attached Nodes	Installed Packages	Custom Attributes	Config Tracking	History
MANAGEMENT INFORMATION							
Name:	<input type="text" value="core.tr3.opsware.com"/>						
Notes:	<input type="text"/>						
IP Address:	172.16.36.18						
OS Version:	Red Hat Enterprise Linux AS 3						
Customer:	<input type="text" value="Opsware"/>						
Facility:	DATACENTER1						
Server Use:	<input type="text" value="Not Specified"/>						
Deployment Stage:	<input type="text" value="Not Specified"/>						
Config Tracking:	<input type="text" value="Disabled"/>						
Console:	(not set)						
Opsware Lifecycle:	Managed						
Server ID:	10003						
Status:	Not Reachable as of Tue May 17 13:11:28 2005						<input type="button" value="Details..."/>

Figure 4-3: Server Properties-Hardware and Additional Information

REPORTED INFORMATION (as of Tue May 17 19:05:57 2005)					
Reporting:	OK				
Agent Version:	30.0.2.102				
Hostname:	core.tr3.opsware.com				
Reported OS:	Linux 3AS				
MAC Address:	00:11:43:D7:2F:5F				
Serial Number:	2YLLP61				
Chassis ID:	2YLLP61				
Manufacturer:	DELL COMPUTER CORPORATION				
Model:	POWEREDGE 1850				
CPUs:	Vendor	Model	Speed	Cache Size	
	GENUINEINTEL	Intel(R) Xeon(TM) CPU 2.80GHz	2793 MHz	1 MB	
	GENUINEINTEL	Intel(R) Xeon(TM) CPU 2.80GHz	2793 MHz	1 MB	
	GENUINEINTEL	Intel(R) Xeon(TM) CPU 2.80GHz	2793 MHz	1 MB	
	GENUINEINTEL	Intel(R) Xeon(TM) CPU 2.80GHz	2793 MHz	1 MB	
Memory:	Type	Capacity			
	RAM	3.9 GB			
	SWAP	1.95 GB			
Storage:	Drive	Media	Capacity	Bus Type	Model
	hda	CDROM	--	IDE	SAMSUNG CD-ROM SN-124
	sda	SCSI DISK	68.24 GB	SCSI	MegaRAID LD 0 RAID0 69G
Network:	See the Network tab				
<input type="button" value="Save"/> <input type="button" value="Cancel"/>					

Software Information

The software that should be installed is recorded in the Opware Model Repository. To access that information, click the Install List or Installed Packages tabs. This shows the software that should be installed on the server or all software that is installed on the server.

To display the list of what software packages should be installed on that server, select the Install List tab from the Manage Servers: Server Properties page.

To display the list of software that is reportedly installed on the server, select the Installed Packages tab from the Managed Servers: Server Properties page.

Partially-installed Solaris packages do not show up in the Installed Packages list, even though the package was partially installed.

Hardware Information

Opware SAS tracks hardware information in a variety of manners. Table 4-1 shows how the Opware Agent obtains the server and hardware information about each managed server.

Table 4-1: Hardware Information that the Opware Agent Reports for Servers

ATTRIBUTE	DESCRIPTION	HOW OBTAINED
Name	The user-configurable name for the server. By default, Opware SAS uses the configured host name of the server until a user edits it.	Windows: Uses the fully qualified DNS name of the server. Linux, Solaris, AIX, HP-UX: Uses the current host name of the server that the <code>hostname</code> command returns.
Reported OS	The version number of the server's operating system.	Windows: Uses the Windows version number as reported by the operating system. This information includes the major version number, the minor version number, the Windows build number, and the Service Pack level. Linux, Solaris, AIX, HP-UX: Uses the operating system version that the <code>uname</code> command returns.
OS Version	The OS version specified for the OS definition.	Specified by the user who prepared the OS with the Prepare Operating System Wizard. See the <i>Opware[®] SAS Policy Setter's Guide</i> for more information.
Serial Number	The serial number of the system. Opware SAS attempts to report a chassis ID, if possible.	Windows, Linux: Obtained from the system BIOS. Solaris, AIX, HP-UX: Obtained from the system ROM.
Manufacturer	The manufacturer of the server if available.	Windows, Linux: Obtained from the system BIOS. Solaris, AIX, HP: Obtained from the system ROM.

Table 4-1: Hardware Information that the Opware Agent Reports for Servers (continued)

ATTRIBUTE	DESCRIPTION	HOW OBTAINED
Model	The model of the server if available.	<p>Windows, Linux: Obtained from the system BIOS.</p> <p>Solaris, AIX: Obtained from the system ROM.</p> <p>HP-UX: Output of model command (which is read from the system ROM).</p>
Memory	The amount of physical RAM and the total amount of virtual memory paging space configured.	<p>Windows: Uses the Windows 2000 API <code>GlobalMemoryStatus()</code>.</p> <p>Linux: Obtained from information in the file <code>/proc/meminfo</code>.</p> <p>Solaris: Obtained from the <code>sysconf</code> and <code>swapctl</code> APIs.</p> <p>AIX: Uses the <code>lsattr</code> command for memory information and the <code>lspv</code> command for paging space.</p> <p>HP-UX: Uses the <code>pstat</code> system call.</p>
Processors	Information about each of the processors in the system.	<p>Windows: If WMI is available, iterates over all instances of <code>Win32_Processor</code>. If WMI is not available, parses the registry key <code>HARDWARE\DESCRIPTION\System\CentralProcessor</code>. There is one sub-key for each processor.</p> <p>Linux: Obtained from information in the file <code>/proc/meminfo</code>.</p> <p>Solaris, HP-UX: Uses system APIs to enumerate the processors in the system.</p> <p>AIX: Uses the <code>lscfg</code> command.</p>
Storage	Information about each installed disk drive or RAID array.	<p>All Platforms: Uses system APIs to discover and probe disk drives and RAID arrays.</p>

Table 4-1: Hardware Information that the Opsware Agent Reports for Servers (continued)

ATTRIBUTE	DESCRIPTION	HOW OBTAINED
Server ID	The internal ID that Opsware SAS uses to identify the server.	In most cases, the server ID is the same as the MID.
MID	The MID (Machine ID) is a unique number that Opsware SAS assigns when the server first registers. The server stores the MID and reports it each time the server registers.	<p>Windows: The MID is stored in the file %ProgramFiles%\Common Files\Loudcloud\cogbot\mid if present.</p> <p>Linux, Solaris, AIX, HP-UX: The MID is stored in the file /var/lc/cogbot/mid.</p>

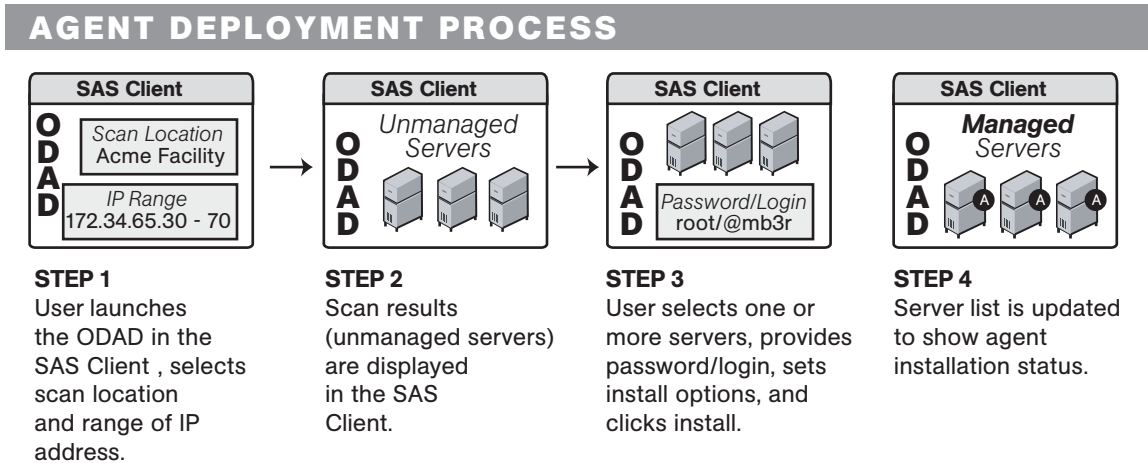
In addition to hardware and software reporting, the Opsware Agent reports networking information. See “Network Configuration” on page 280 in Chapter 7 for descriptions of the networking information reported and how you can modify that information using the Network tab in the SAS Web Client.

Opsware Discovery and Agent Deployment

The Opsware Discovery and Agent Deployment (ODAD) feature helps to deploy Opsware Agents to a large number of servers through the Opsware SAS Client (SAS Client). This feature helps to identify servers on which to install an Opsware Agent, specify the

deployment actions to be carried out on each server, select the login protocols to connect to each server, specify the Opware Agent Installer options for installing an Opware Agent, and generate reports on Opware Agent installation status. See Figure 4-4.

Figure 4-4: Agent Deployment Process



This overview section contains the following topics:

- Discovering Servers for Installing an Opware Agent
- Setting Deployment Actions for Each Server
- Specifying Login Settings
- Opware Agent Installer Options
- Reports on Server Status

See “Installing Opware Agents Using ODAD” on page 116 in this chapter for information about how to install an Opware Agent.

Discovering Servers for Installing an Opware Agent

Using the Opware Discovery and Agent Deployment feature, you can select a location to scan for servers. After selecting a location, you can specify the IP addresses or IP address ranges to perform a network scan to identify servers in which to install an Opware Agent. Instead of performing a network scan, you can also import a file containing a list of IP addresses or IP address ranges. When the scan is complete, a list of scanned servers is shown.

For each server, this feature determines the status of the server, its IP address, its host name, detected operating system, and open ports used to connect to the server.

- [Setting Deployment Actions for Each Server](#)
- [Specifying Login Settings](#)
- [Opware Agent Installer Options](#)
- [Reports on Server Status](#)

Setting Deployment Actions for Each Server

Once you have identified the servers, you can select the servers and perform the following deployment actions:

- Verify installation prerequisites.

When you select this action, verification checks are performed to ensure that the Opware Agent is successfully installed on the server. The verification checks include:

- Checking for sufficient disk space for Opware Agent installation on the server
 - Verifying that no other application is using port 1002
 - Verifying if ports to the Opware Gateway are accessible
- Verify prerequisites, and copy the Opware Agent Installer to servers.

When you select this action, verification checks are performed to ensure that the Opware Agent is successfully installed on the server and the Opware Agent Installer is copied to the server.

- Verify prerequisites, copy installer, and install Opware Agent.

When you select this action, verification checks are performed to ensure that the Opware Agent is successfully installed on the server, the Opware Agent Installer is copied to the server, and the Opware Agent is installed on the server.

- [Discovering Servers for Installing an Opware Agent](#)
- [Specifying Login Settings](#)
- [Opware Agent Installer Options](#)
- [Reports on Server Status](#)

Specifying Login Settings

After selecting the deployment action, you can select the network protocols to connect to the server and specify the user name and password to login to each server. The Opsware Agent needs administrator-level privileges (root on Unix servers and administrator on Windows servers) to manage a server. Therefore, Opsware Agent installation is performed as root on Unix operating systems and as administrator on Windows operating systems. ODAD tries to log into each of the selected servers with the specified user name and password and performs the specified deployment actions.

- [Discovering Servers for Installing an Opsware Agent](#)
- [Setting Deployment Actions for Each Server](#)
- [Opsware Agent Installer Options](#)
- [Reports on Server Status](#)

Opsware Agent Installer Options

The Opsware Discovery and Agent Deployment feature allows you to specify the installer options listed in Table 4-2.

Table 4-2: Opsware Agent Installer Options

OPTION	DESCRIPTION
Start the Opsware Agent after Installation	Starts the Opsware Agent after installing it on the server. By default, the Opsware Agent Installer does not start the Opsware Agent.
Remove existing machine IDs and cryptographic material	Removes any existing machine specific identifying material such as Machine ID file (MID), and all machine-specific cryptographic material from the server.
Ignore prerequisite check failures	Ignores the prerequisite check failures and forces Opsware Agent installation.
Set the server's time from the Opsware core	Synchronizes the time on the server in which the Opsware Agent is installed to the Opsware core.

Table 4-2: Opsware Agent Installer Options (continued)

OPTION	DESCRIPTION
Install Windows Installer (MSI) if required	Installs MSI along with the Opsware Agent. If MSI is already installed, this option has no effect.
Install Windows Management Instrumentation (WMI) if required	Installs WMI along with the Opsware Agent. If WMI is already installed, this option has no effect.
Reboot Windows servers after agent installation	Reboots windows servers after Opsware Agent installation is complete.
Install Red Hat Package Manager (RPM) on AIX and Solaris	Installs the RPM handler with the Opsware Agent. Always include this option when you install Opsware Agents on Solaris and AIX servers.
Reset Opsware Agent configuration, if present	Replaces the existing Opsware Agent configuration.
Delete gateway address list, if present	Deletes the Opsware Gateway address list if present and is no longer required.
Overwrite staged Opsware Agent installer	Overwrites the existing Opsware Agent Installer.
Log Level	Sets the log level for log messages. With this option, you can specify the log levels of error, warning, info, and trace.
Use Opsware Gateways	Specifies the Opsware Gateways used during Opsware Agent installation.
Immediately do a full hardware registration	Forces the Opsware Agent Installer to report full hardware information to the Opsware core.
Immediately do software registration	Forces the Opsware Agent Installer to report full software information to the Opsware core.

Table 4-2: Opsware Agent Installer Options (continued)

OPTION	DESCRIPTION
Suppress Opsware Agent reachability check	By default, the installer triggers the core to check if the server is reachable. This option disables this check during installation.
Disallow anonymous SSL connections if Opsware Agent is dormant	Configures the Opsware Agent so that browsers cannot connect without a valid certificate.
Force creation of new device record if conflict found	During registration, the Data Access Engine creates a new device record. This option suppresses this functionality.
Fail if initial hardware registration fails (do not go dormant)	Does not allow the Opsware Agent to become dormant, if it fails to report hardware information.
Do not open Windows Firewall for core-agent communications	By default, the Opsware Agent Installer will modify the Windows Firewall configuration on Windows XP and Windows 2003 (r2) servers to allow the Opsware core to contact the managed server on port 1002. If you select this option, the firewall configuration will not be modified. The server may not be manageable by Opsware in this case.
Remediate software policies	Remediates the server against any software policies attached to the server.
Attach to software Policy ID	Attaches server to the software policy <ID>.
Extra Installer options	Allows you to specify any other installer options.

Table 4-2: Opsware Agent Installer Options (continued)

OPTION	DESCRIPTION
Install directory (UNIX)	Allows you to specify the directory where the Opsware Agent will be installed. By default, the Agent is installed in <code>/opt/opsware/agent</code> on UNIX, and <code>%ProgramFiles%\Opsware\agent</code> on Windows.

- [Discovering Servers for Installing an Opsware Agent](#)
- [Setting Deployment Actions for Each Server](#)
- [Specifying Login Settings](#)
- [Reports on Server Status](#)

Reports on Server Status

After the deployment action is complete, the SAS Client displays the results and updates the status icons for the servers as shown in Table 4-3.

Table 4-3: Server Status








ICONS	SERVER STATUS
	The server is unmanaged.
	The server is managed by Opsware.
	The server failed prerequisite checks.

Table 4-3: Server Status (continued)

ICONS	SERVER STATUS
	The server passed prerequisite checks.
	The server passed prerequisite checks and the Opware Agent Installer was copied to the server.
	The Opware Agent was successfully deployed.
	The Opware Agent was not successfully deployed.



A server is considered to be managed by Opware when the ODAD determines that the Opware Agent is listening for TCP connections on port 1002.

For a failed deployment action, you can view the errors on each server. You can also log into the server from this feature and correct the errors.

Using this feature, you can create the following reports:

- All the servers in the current network scan
- Selected servers in the current network scan
- All the servers in the current network scan with successful deployments
- Servers in the current network scan with failed deployments

You can save and export the reports to a CSV, HTML, or text format file.

- [Discovering Servers for Installing an Opware Agent](#)
- [Setting Deployment Actions for Each Server](#)

- [Specifying Login Settings](#)
- [Opware Agent Installer Options](#)

Opware Agent Installation Using ODAD

The Opware Discovery and Agent Deployment (ODAD) feature helps you to deploy Opware Agents to a large number of servers through the SAS Client. This section contains the following topics:

- Prerequisite Setup for Opware Discovery and Agent Deployment
- Permissions Required for Opware Discovery and Agent Deployment
- Installing Opware Agents Using ODAD

Prerequisite Setup for Opware Discovery and Agent Deployment

Before you can install Opware Agents using ODAD, you must install the Windows Agent Deployment Helper package (required for installing Opware Agents on Windows server only) and install JRE version 1.4.2_10 for running the SAS Client.

See the *Opware[®] SAS Planning and Installation Guide* for more information about installing the Windows Agent Deployment Helper Package.

See “Requirements for Running the SAS Client” on page 72 in Chapter 3 for information about installing JRE.

- [Permissions Required for Opware Discovery and Agent Deployment](#)
- [Installing Opware Agents Using ODAD](#)

Permissions Required for Opware Discovery and Agent Deployment

To use the Opware Discovery and Agent Deployment feature you must have certain permissions. See *Opware[®] SAS Administration Guide* for more information about the permissions required to use the ODAD feature.

To obtain the required permissions for scanning and deploying Opware Agents, contact your Opware administrator.

- [Prerequisite Setup for Opware Discovery and Agent Deployment](#)
- [Installing Opware Agents Using ODAD](#)

Installing Opsware Agents Using ODAD

To install Opsware Agents using ODAD, launch the SAS Client from the Opsware SAS Web Client. See “Installing and Launching the SAS Client” on page 72 in Chapter 3 for more information.

Perform the following steps to install an Opsware Agent:

- 1** Log into the SAS Client. The SAS Client Page appears.
- 2** From the navigation pane, select Devices and then select Unmanaged Servers.
- 3** Select a location to scan for servers from the Scan in drop-down list.
- 4** Select Supply IP Address Ranges from the drop-down list to specify a set of IP address ranges to scan. Enter the IP address range in the From and To field. Click the plus (+) button (next to the To field) to add another IP address range. You can add a maximum of five IP address ranges. Click the minus (-) button to delete the IP address range field.

Or

Select Explicit list of IPs from the drop down list to specify the list of IP addresses to scan. Click the ellipsis (...) button as shown in Table 4-5 to display a text editor that allows you to load and scan a file with IP ranges to scan.

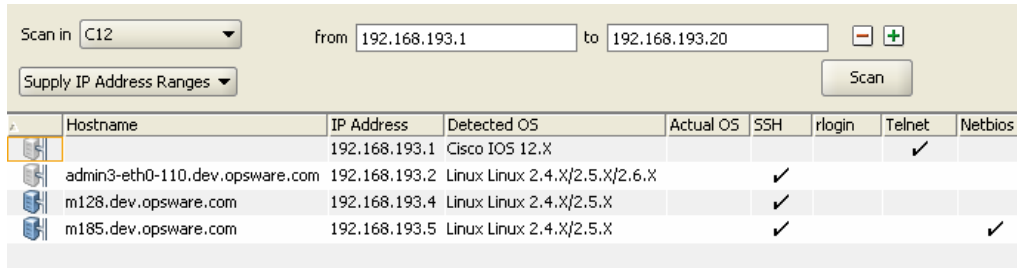
Figure 4-5: Loading a File with IP Addresses



- 5** Click **Scan** to scan for servers. When the scan is complete, the list of scanned servers is shown. For each server, ODAD determines the status of the server, its IP address, its host name, the detected operating system, the actual operating system,

and open ports that can be used to connect to the server. See Figure 4-6. The actual operating system of the server can be only determined if ODAD is able to successfully log into the server.

Figure 4-6: Scan Results

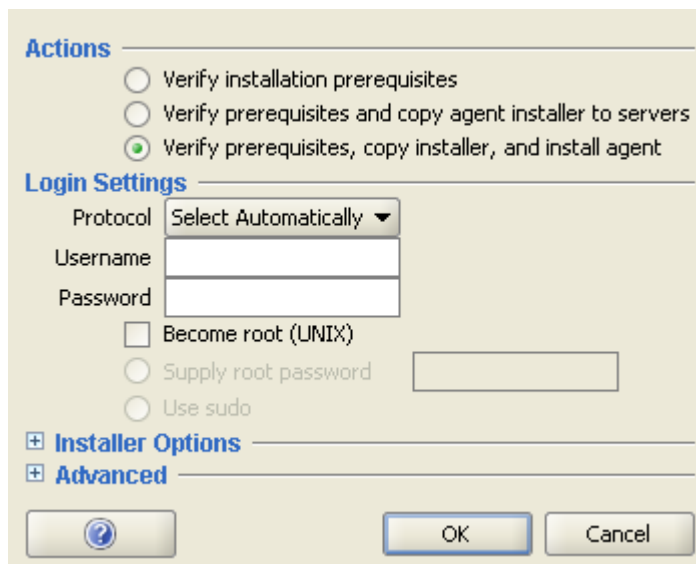


The screenshot shows a web interface for scanning servers. At the top, there are input fields for 'Scan in' (set to 'C12'), 'from' (192.168.193.1), and 'to' (192.168.193.20). There is a 'Scan' button and a 'Supply IP Address Ranges' dropdown. Below is a table with the following data:

	Hostname	IP Address	Detected OS	Actual OS	SSH	rlogin	Telnet	Netbios
		192.168.193.1	Cisco IOS 12.X				✓	
	admin3-eth0-110.dev.opsware.com	192.168.193.2	Linux Linux 2.4.X/2.5.X/2.6.X		✓			
	m128.dev.opsware.com	192.168.193.4	Linux Linux 2.4.X/2.5.X		✓			
	m185.dev.opsware.com	192.168.193.5	Linux Linux 2.4.X/2.5.X		✓			✓

- 6 Click on any of the column headings to sort the server list by that column. If you want to hide managed servers, select **Hide Opsware-managed Servers** from the **View** menu.
- 7 Select servers on which you want to deploy the Opsware Agent. The SAS Client supports hot keys to make multiple selections.
- 8 From the **Actions** menu, select **Deploy Agent**. The Deploy Agent dialog box appears as shown in Figure 4-7.

Figure 4-7: Deploy Agents



The screenshot shows the 'Deploy Agent' dialog box. It has several sections:

- Actions:** Three radio buttons:
 - Verify installation prerequisites
 - Verify prerequisites and copy agent installer to servers
 - Verify prerequisites, copy installer, and install agent
- Login Settings:**
 - Protocol: Select Automatically (dropdown)
 - Username: [text input]
 - Password: [text input]
 - Become root (UNIX)
 - Supply root password [text input]
 - Use sudo
- Installer Options:** [expanded section]
- Advanced:** [expanded section]

At the bottom, there are buttons for '?', 'OK', and 'Cancel'.

9 Select one of the following deployment actions:

- Verify installation prerequisites.
- Verify prerequisites and copy agent installer to servers.
- Verify prerequisites, copy installer, and install agent.

See “Setting Deployment Actions for Each Server” on page 109 in this chapter for more information.

10 Select a network protocol to log in and connect to the server from the drop-down list.

Or

Choose Select Automatically to allow ODAD to select an appropriate protocol for each server.

11 Enter the user name to log into the server. For Windows, log in as administrator. For Unix, log in as root.

12 If root logging is not allowed, select the Become root (UNIX) checkbox. Select “Supply root password” and enter the password or select Use sudo, if sudo access is enabled for that account.

See “Specifying Login Settings” on page 110 in this chapter for more information.

13 Specify the Opsware Agent Installer options to control the way the Opsware Agent is installed on a server. See “Opsware Agent Installer Options” on page 110 in this chapter for more information.

14 Click **OK** to deploy Opsware Agents to selected servers.

15 After the deployment action is completed, the SAS Client displays the results and updates the status icons for the servers. You can view information on an unmanaged server and generate reports on Opsware Agent Installation status. See “Reports on Opsware Agent Installation” on page 123 in this chapter for more information.

- [Opsware Discovery and Agent Deployment](#)
- [Opsware Agent Installation Using ODAD](#)
- [Viewing Unmanaged Server Information](#)

Viewing Unmanaged Server Information

After the deployment action is completed, you can review the results and generate reports. You can view the summary and history information for an unmanaged server. For a failed deployment action, you can view the errors on each server. You can also log into the server from ODAD and correct the errors.

This section discusses the following topics:

- Summary Information for an Unmanaged Server
- History Information for an Unmanaged Server
- Remote Terminal Sessions on Unmanaged Servers
- Reports on Opsware Agent Installation

Summary Information for an Unmanaged Server

The Unmanaged Server Summary browser shows the following information about the unmanaged server:

- **Host Name:** The host name of the unmanaged server, if defined in the Domain Name System (DNS).
- **IP Address:** The IP address of the unmanaged server.
- **Detected OS:** The operating system detected on the server after performing the network scan.
- **Actual OS:** The actual operating system detected on the server after the deployment action.
- **MAC Address:** The Media Access Control (MAC) address, which is the network interface card's unique hardware number of the unmanaged server. The MAC is used as the server's physical address on the network. The MAC address is only detected if the server is on the same physical network as the Opsware Gateway.
- **NIC Vendor:** The vendor name for the Network Interface Card (NIC) driver. The NIC vendor is only detected if the server is on the same physical network as the Opsware Gateway.
- **Open Ports:** The available open ports on an unmanaged server.
- **Number of Deployment Attempts:** The number of deployment attempts on an unmanaged server.

- **Last Deployment Attempt Date/Time):** The Date/Time of the last deployment attempt.
- **Last Deployment Attempt Message:** The message stating the possible cause for the failure of the last deployment attempt.

Viewing Summary Information of an Unmanaged Server

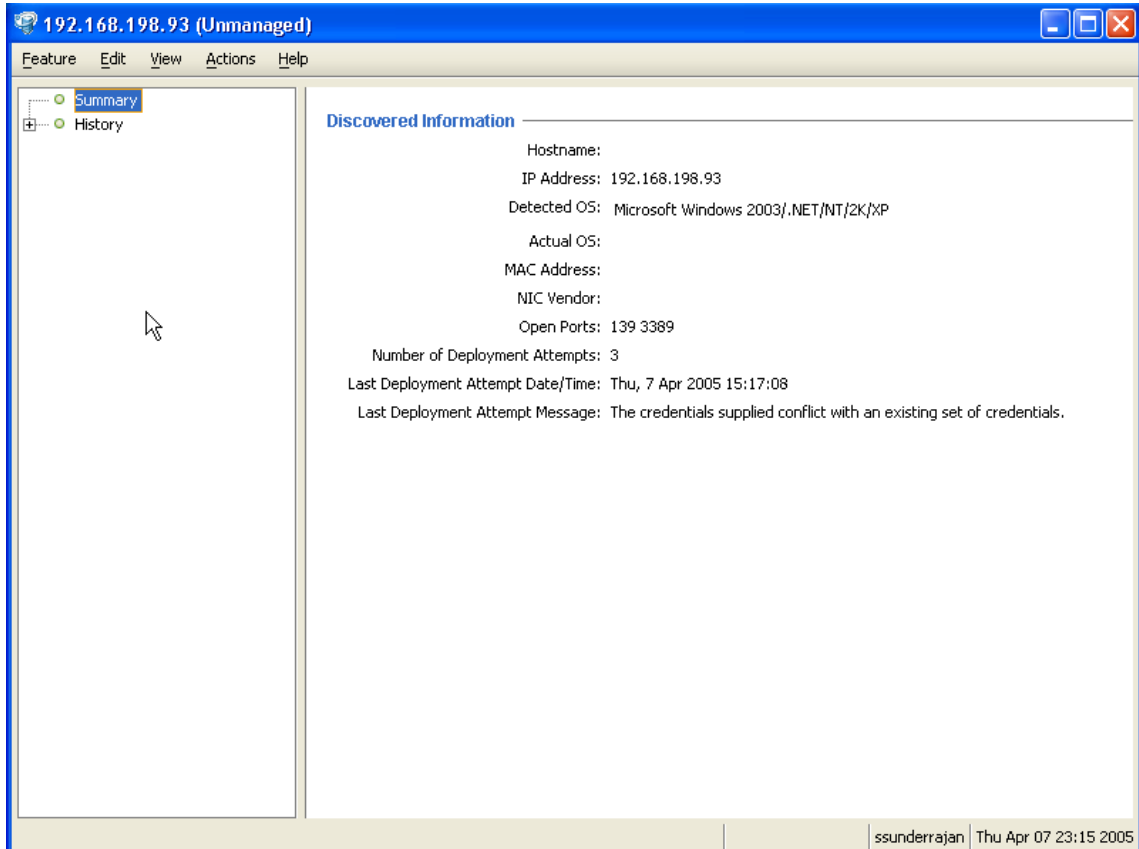
Perform the following steps to view the summary of an unmanaged server.

- 1** Log into the SAS Client. The SAS Client Page appears.
- 2** From the navigation pane, select Devices and then select Unmanaged Servers.
- 3** From the Unmanaged Servers page, select the unmanaged server. From the **Actions** menu, select **Open**.

The Unmanaged Server Browser page appears.

- 4 Click Summary on the left side navigation panel of the Unmanaged Server Browser page to view the summary on the unmanaged server. See Figure 4-8.

Figure 4-8: Unmanaged Server Summary Page



- [Viewing Unmanaged Server Information](#)
- [History Information for an Unmanaged Server](#)
- [Remote Terminal Sessions on Unmanaged Servers](#)
- [Reports on Opsware Agent Installation](#)

History Information for an Unmanaged Server

The Unmanaged Server History Browser shows a history of all actions executed on unmanaged servers such as:

- A summary of the actions performed on the unmanaged server
- Details of all the actions performed on the unmanaged server

- Log information

The history is read-only.

Viewing History Information of an Unmanaged Server

Perform the following steps to view the history of an unmanaged server:

- 1** Log into the SAS Client. The SAS Client Page appears.
- 2** From the navigation pane, select Devices and then select Unmanaged Servers.
- 3** From the Unmanaged Servers page, select the unmanaged server. From the **Actions** menu, select **Open**.

The Unmanaged Server Browser page appears.

- 4** Click History on the left side navigation panel of the Unmanaged Server Browser page to view the history of all actions executed on unmanaged servers.

- [Viewing Unmanaged Server Information](#)
- [Summary Information for an Unmanaged Server](#)
- [Remote Terminal Sessions on Unmanaged Servers](#)
- [Reports on Opsware Agent Installation](#)

Remote Terminal Sessions on Unmanaged Servers

Using the ODAD feature, you can open terminal sessions on an unmanaged server. You can log into the server using the appropriate protocol to correct the errors on the server or perform any other operations.

You can use the SAS Client Remote Terminal and Shell preferences to configure the Terminal (UNIX) and RDP (Windows) clients used to launch terminal sessions. See “Overview of the Global Shell” on page 375 in Chapter 10 for more information.

Opening Remote Terminal Sessions on an Unmanaged Servers

Perform the following steps to open remote terminal sessions on a server:

- 1** Log into the SAS Client. The SAS Client Page appears.
- 2** From the navigation pane, select Devices and then select Unmanaged Servers.
- 3** From the Unmanaged Servers page, select the unmanaged server. From the **Actions** menu, select the appropriate log in with protocol.

- [Viewing Unmanaged Server Information](#)
- [History Information for an Unmanaged Server](#)
- [Summary Information for an Unmanaged Server](#)
- [Reports on Opware Agent Installation](#)

Reports on Opware Agent Installation

Using the Opware Discovery and Agent Deployment feature, you can create the following reports:

- All the servers in the current network scan
- Selected servers in the current network scan
- Servers in the current network scan with successful deployments
- Servers in the current network scan with failed deployments

You can also save and export the reports to a CSV, HTML, or text file format.

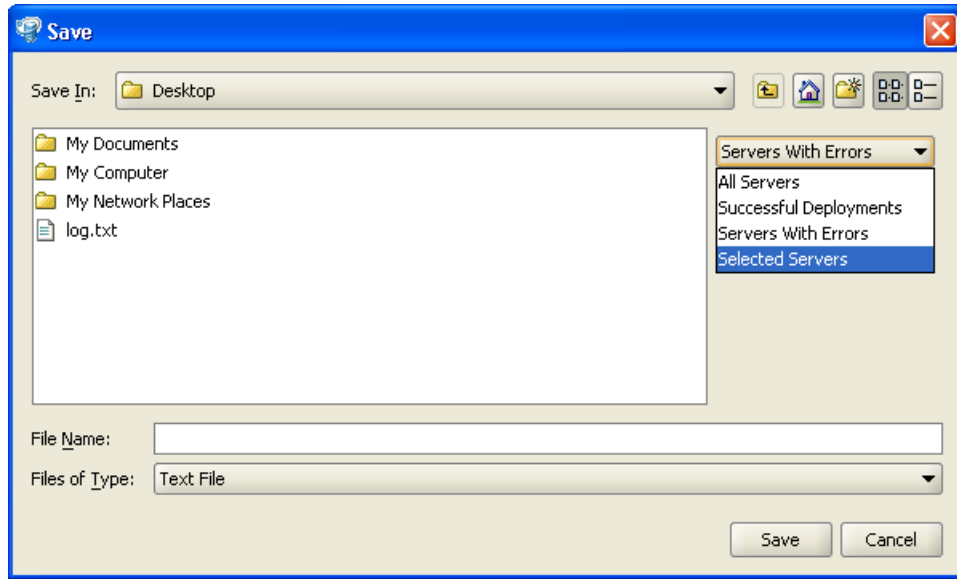
Creating Reports on Opware Agent Installation

Perform the following steps to create reports:

- 1** Log into the SAS Client. The SAS Client Page appears.
- 2** From the navigation pane, select Devices and then select Unmanaged Servers.
- 3** From the Unmanaged Servers page, select the unmanaged server. From the **Actions** menu, select **Export to** the desired report format. The Save Report dialog box appears.

- From the drop-down list, select the type of report as shown in Figure 4-9.

Figure 4-9: Generating Reports



- Enter the location and file name to save the report.

Example Report

The following example shows a report of servers with failed deployments.

Servers which the Opsware Agent could not be deployed to:

Hostname : Unknown

IP Address : 192.168.198.93

Detected Operating System : Microsoft Windows 2003 Server or XP SP2

Open Ports : 139 3389

MAC Address : Unknown

NIC Vendor : Unknown

of Deployment Attempts : 2

Last Deployment Message : The credentials supplied conflict with an existing set of credentials.

Last Deployment Attempt Date/Time : "Wed, 6 Apr 2005 16:18:46"

Failed Phase : Check

Return Code : 2013

Suggested Resolution : The Agent Deployment Helper was unable to log in to the unmanaged server.

An incorrect login name or password was specified. Try a different login name and/or password.

- [Summary Information for an Unmanaged Server](#)
- [History Information for an Unmanaged Server](#)
- [Remote Terminal Sessions on Unmanaged Servers](#)

Agent Reachability Communication Tests

This section provides information on agent reachability Communication Tests within Opsware SAS and contains the following topics:

- Overview of Communication Tests
- Communication Tests and Unreachable Opsware Agents
- Communication Test Types
- Communication Test Errors
- Additional Information on Communication Tests
- Running a Communication Test on an Individual Server
- Running a Communication Test on Multiple Servers
- Viewing Servers by Communication Status
- Searching for Unreachable Servers
- Creating Communication Test DCI Reports
- Viewing My Jobs Communication Tests
- Exporting the Unreachable Server Status List to CSV

Overview of Communication Tests

Sometimes an Opsware Agent can become unreachable, which means that the SAS Web Client has difficulty communicating with the Opsware Agent. When an Opsware Agent is unreachable, the server it is installed on is considered unmanaged. This section explains how to use the Communication Test to find unreachable Opsware Agents and suggests ways that you can resolve these problems.

To help identify those managed servers that have unreachable agents, the SAS Web Client runs periodic Communication Tests to verify that Opsware SAS can communicate with all servers under its management. You can always check the reachability of Opsware Agents by looking at the server's properties, or by viewing the current agent reachability status for all managed servers since the last Communication Test was run by choosing the Communication view from the Manage Servers list.

To determine the current reachability of a specific Opsware Agent, you can run a Communication Test to find those servers that have unreachable agents by using the Communication Test feature located in the Server menu of the Manage Server list. A Communication Test lists all servers with unreachable agents, returns specific errors associated with each unreachable Opsware Agent, and provides troubleshooting information to help you get the Opsware Agent back in working order.

You have the ability to check Opsware Agent reachability for individual servers, selected servers, or all servers under management of Opsware SAS. Each time that you run a Communication Test, this test is saved in the My Jobs panel, which allows you to view a history of all the Communication Tests that you have run. You can even export the current reachability status of all managed servers to a CSV file.

Communication Tests and Unreachable Opsware Agents

The Communication Test works by testing communication and data exchange between the specific components of the Opsware core and each managed server. The Opsware core is the entire collection of servers and services that provide Opsware services. In order to successfully manage servers, the Opsware core needs to be able to communicate with each Opsware Agent on all servers under Opsware SAS management.

Communication Test Types

The Communication Test performs the following diagnostics to determine if an Opsware Agent is reachable:

- **Command Engine to Agent Communication (AGT):** Determines if the Command Engine can communicate with the agent. The Command Engine is the Opware SAS component that enables distributed programs to run across many servers. The Command Engine handles the entry of scripts into the Opware Model Repository (the script storage location in Opware SAS) and the versioning of stored scripts.
- **Crypto Match (CRP):** Checks that the SSL cryptographic files that the agent uses are valid.
- **Agent to Command Engine Communication (CE):** Verifies that the agent can connect to the Command Engine and retrieve a command for execution.
- **Agent to Data Access Engine (DAE):** Checks whether or not the agent can connect to the Data Access Engine and retrieve its device record. The Data Access Engine provides an XML-RPC interface to the Model Repository that simplifies interaction with various clients such as the SAS Web Client, system data collection, and monitoring agents on servers.
- **Agent to Software Repository Communication (SWR):** Determines if the agent can establish an SSL connection to the Software Repository. The Software Repository is the central repository for all software that Opware SAS manages. It contains software packages for operating systems, applications, databases, customer code, and software configuration information.
- **Machine ID Mismatch (MID):** Checks that the Machine ID (MID) on the server matches the MID registered in the Model Repository for the agent.

When the test finishes, it returns results that show either success or failure for each test run on each server. For each failed test, the nature of the failure is indicated in the Test Summary column of the Communication Test results page. In some cases, the failure of one test might prevent other tests from being executed.

See “Opware Agent Functionality on Managed Servers” on page 102 in this chapter for information about the Opware Agent and its relationship to managed servers.

Communication Test Errors

After you run a Communication Test, three icons indicate the success or failure of agent reachability as Table 4-4 shows.

Table 4-4: Agent Unreachability Status Icons




STATUS ICON	DESCRIPTION
	Communication Test passed. Agent is reachable.
	Communication Test unable to be executed.
	Communication Test failed. Agent is unreachable.

Table 4-5 describes each type of Communication Test and all possible errors for each test.

Table 4-5: Communication Test Types with Possible Results

TEST	DESCRIPTION	RESULTS
Command Engine to Agent Communication (AGT)	Determines if the Command Engine can communicate with the agent	<ul style="list-style-type: none"> 1 OK 2 Untested 3 Unexpected error 4 Connection refused 5 Connection time-out 6 Request time-out 7 Server never registered 8 Realm is unreachable 9 Tunnel setup error 10 Gateway denied access 11 Internal gateway error 12 Gateway could not connect to server 13 Gateway time-out
Crypto Match (CRP)	Checks that the agent's SSL cryptographic files are valid	<ul style="list-style-type: none"> 1 OK 2 Untested 3 Unexpected error 4 Agent certificate mismatch 5 SSL negotiation failure

Table 4-5: Communication Test Types with Possible Results (continued)

TEST	DESCRIPTION	RESULTS
Agent to Command Engine Communication (CE)	Verifies that the agent can connect to the Command Engine and retrieve a command for execution	1 OK 2 Untested 3 Unexpected error 4 Connection refused 5 Connection time-out 6 DNS does not resolve 7 Old agent version 8 Realm is unreachable 9 No gateway defined 10 Tunnel setup error 11 Gateway denied access 12 Gateway name resolution error 13 Internal gateway error 14 Gateway could not connect to server 15 Gateway time-out 16 No callback from agent

Table 4-5: Communication Test Types with Possible Results (continued)

TEST	DESCRIPTION	RESULTS
Agent to Data Access Engine (DAE)	Checks whether or not the agent can connect to the Data Access Engine and retrieve its device record	1 OK 2 Untested 3 Unexpected error 4 Connection refused 5 Connection time-out 6 DNS does not resolve 7 Old agent version 8 Realm is unreachable 9 No gateway defined 10 Tunnel setup error 11 Gateway denied access 12 Gateway name resolution error 13 Internal gateway error 14 Gateway could not connect to server 15 Gateway time-out

Table 4-5: Communication Test Types with Possible Results (continued)

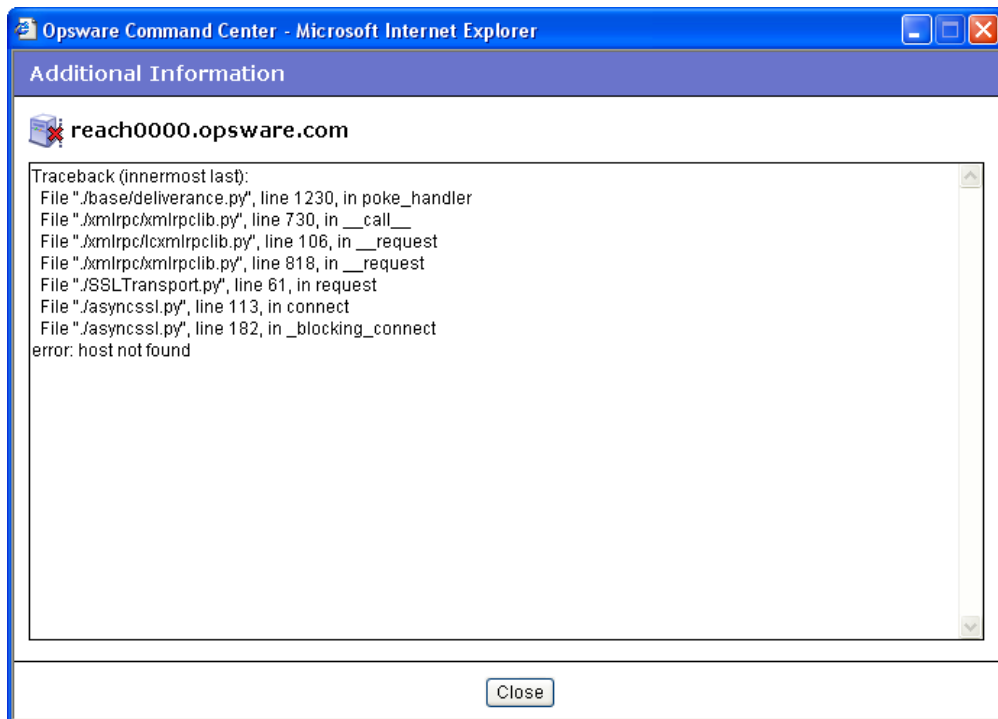
TEST	DESCRIPTION	RESULTS
Agent to Software Repository Communication (SWR)	Determines if the agent can establish an SSL connection to the Software Repository	<ul style="list-style-type: none"> 1 OK 2 Untested 3 Unexpected error 4 Connection refused 5 Connection time-out 6 DNS does not resolve 7 Old agent version 8 Server identification error 9 Realm is unreachable 10 No gateway defined 11 Tunnel setup error 12 Gateway denied access 13 Gateway name resolution error 14 Internal gateway error 15 Gateway could not connect to server 16 Gateway time-out
MID Match	Checks that the Machine ID (MID) on the server matches the MID registered in the Model Repository for the agent	<ul style="list-style-type: none"> 1 OK 2 Untested 3 Unexpected error 4 MID Mismatch

See “Communication Test Troubleshooting” in *Opware® SAS User's Guide: Server Automation* for information about how to troubleshoot Communication Test Errors.

Additional Information on Communication Tests

In the case that the Communication Test cannot be performed on a server, you see an error named Unexpected Error with a small plus (+) button next to it. Click the plus (+) button to see the Additional Information window, which provides traceback information regarding the error. You can send this information to Opsware Customer Support to solve a problem of this nature. See Figure 4-10.

Figure 4-10: Additional Information on an Unexpected Error



Running a Communication Test on an Individual Server

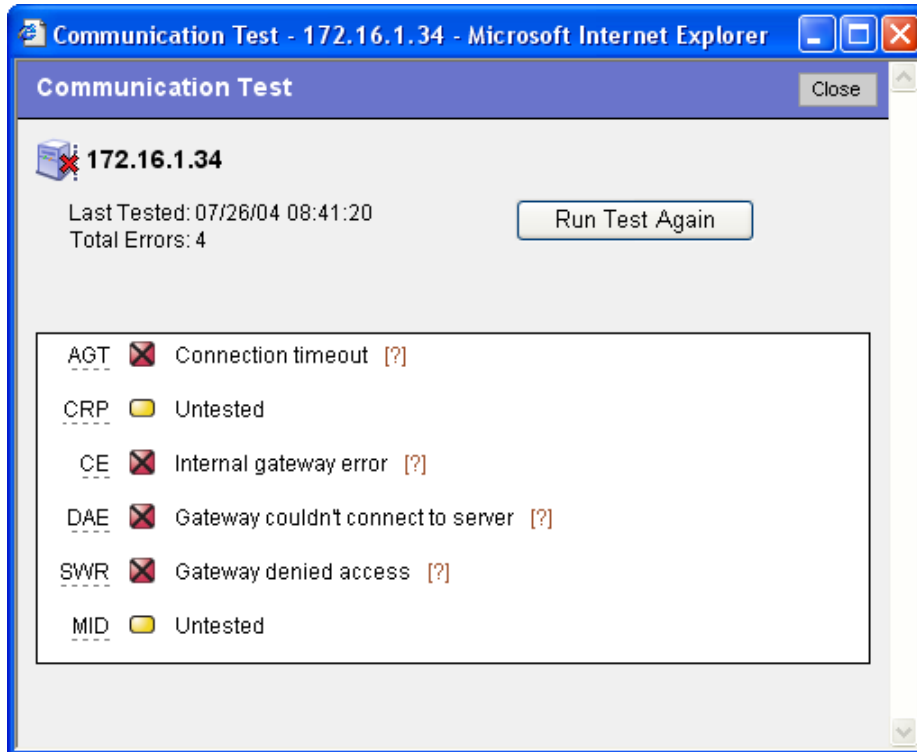
Perform the following steps to run a Communication Test on an individual server to find out if the Opsware Agent on that server is reachable:

- 1** From the navigation panel, click Servers ► Manage Servers.
- 2** From the Manage Servers list, click the display name of the server that you want to perform a Communication Test on.

On the Server Property page, look in the Status field and notice that the server is either listed as Reachable or Not reachable. If listed as Not Reachable, a date indicates when the last regularly scheduled Communication Test was performed.

- 3 To see the results of the last Communication Test for this server, click **Details**. The Communication Test window for the server appears, as Figure 4-11 shows.

Figure 4-11: Communication Test Results on an Individual Server



The results listed in this window show details from when the last regularly scheduled Communication Test was run.

- 4 To view troubleshooting information for any of the test errors, move your mouse over the error name (for example SWR). When your mouse cursor changes to a question mark, click the question mark to view the troubleshooting help.
- 5 To rerun the Communication Test, click **Run Test Again**. The new results display in the same window when the test finishes.

Running a Communication Test on Multiple Servers

Perform the following steps to run a Communication Test on multiple servers and to find out which managed servers are not reachable:

- 1 From the navigation panel, click Servers ► Manage Servers.

- 2 In the Manage Servers Summary View page, select the servers for which you want a Communication Test.
- 3 Choose **Tasks > Run > Communication Test**. The Communication Test window opens and the test is initiated. The top of the test window shows the status report for the Communication Test, which indicates the time of the test, how many servers in the test were reachable, which servers were not reachable, and a progress bar. This summary information is shown in Figure 4-12.

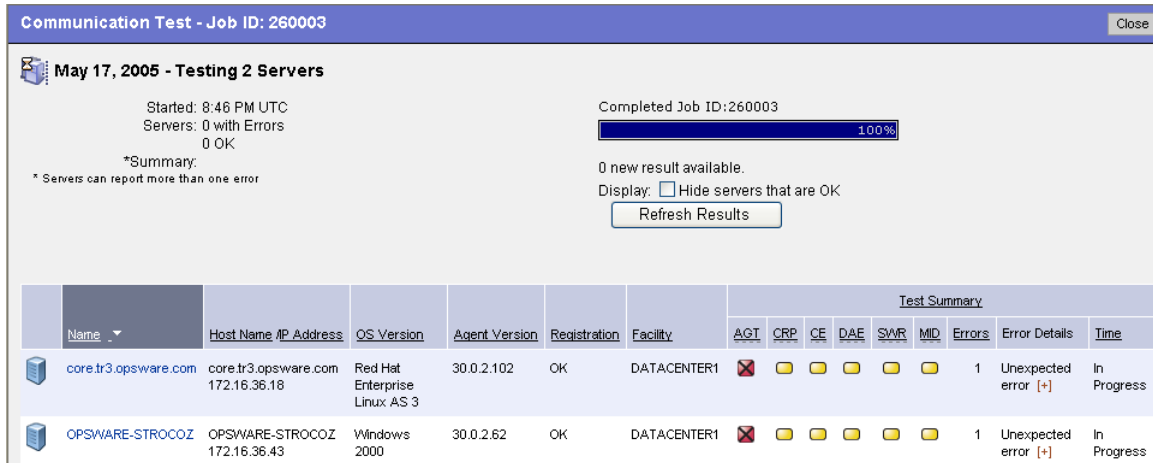
Figure 4-12: Communication Test Summary



- **Date:** Provides the date of the test.
- **Statistics:** Shows start and finish time, total servers OK, total servers with unreachable agents, and a summary of errors.
- **Progress Bar:** Provides live feedback of Communication Test progress. Progress data includes the number of servers completed, the total number of servers to be completed, and the list of servers completed so far.
- **Refresh Results Button:** Refreshes the results screen with new results.

Below the summary section is a list of all Opware Agents that were not reachable and their details, as Figure 4-13 shows.

Figure 4-13: Communication Test Results on an Unreachable Agent



- The results section shows a table of all unreachable servers, detailing server name, host name/IP address, OS, Opware Agent version, registration (when the Opware Agent last reported to Opware SAS), and the time the test was completed.
- Click the title of each column to sort the test information by specific categories.
- The Test Summary section shows a list of all Communication Test types that were run, and which errors were returned. For information about each type of error and how to troubleshoot Opware Agent reachability problems, click the link on each error to view online help.

Viewing Servers by Communication Status

Perform the following steps to view all manage servers with the most recent Communication Test results for each manage server:

- 1 From the navigation panel, click Servers ► Manage Servers.
- 2 From the **View** menu, choose **Communication**. A list of the most recent Communication Test that was run on all managed servers appears. All servers listed in this view are listed as unreachable or reachable since the last regularly scheduled Communication Test was run.

- 3** To sort the information in this view, click any of the column headings. For example, you might want to view the servers by number of errors. Click the Error column title by name, by OS version, and so on.
- 4** To export this view to the CSV file format, choose **Export to CSV** from the **Resource** menu.
- 5** To run a new Communication Test for some or all of the servers in this view, select the servers that you want to run a Communication Test on and then choose **Run ► Communication Test** from the **Tasks** menu.

Searching for Unreachable Servers

Another way you can discover unmanaged servers (those with unreachable agents) is to search for all servers that have a status of unreachable. See “Using the Search Feature” on page 171 in *Opsware® SAS User’s Guide: Server Automation* for more information.

Perform the following steps to search for unreachable agents:

- 1** From the navigation panel, click Servers ► Server Search. The Server Search page appears.

- 2 From the Server Search page, choose the Agent Reporting attribute from the first list, as Figure 4-14 shows.

Figure 4-14: Agent Reporting Server Search Attribute



More criteria displays for the search parameters.

- 3 From the far right list of search attributes, select Not Reporting. Your search parameters are Agent Status is Not Reporting.
- 4 Click **Search**. Wait a few moments for the results (the speed of the search results depends on how many managed servers are being searched). If any of your managed servers are not reachable, these servers will be listed in the search results.
- 5 To run a new Communication Test on these servers, select the server (check box next to the server), and choose **Run ► Communication Test** from the **Tasks** menu.

Creating Communication Test DCI Reports

To view a Communication Test in a report format, you can use the Data Center Intelligence (DCI) Reporting feature. It enables you to create a printable report of the Communication Test results. After you make a report of the test results, you can export the report to HTML, CSV, Microsoft Word, and other file formats, so that you can exchange the report with others.

For information on how to create a DCI Communication Test report, view the DCI online help by clicking Help in the SAS Web Client.

Viewing My Jobs Communication Tests

Each time that you run a Communication Test, the information is saved as a My Job. This feature automatically saves a history of all tests that you run. To view saved Communication Tests, perform the following steps:

- 1** From the navigation panel, click My Job.
- 2** From the My Job list, click the Communication Test job that you want to view.
- 3** In the Communication Test window, wait a few moments for the Communication Test information to load, then click **View Details**. You see the Communication Test window.

Exporting the Unreachable Server Status List to CSV

Perform the following steps to export the list of all servers that have a status of unreachable to the CSV file format:

- 1** From the navigation panel, click Servers ► Manage Servers.
- 2** From the **View** menu, choose **Communication**. You see a list of all servers that are in an unreachable or reachable state.

To export a list of these servers to the CSV file format, select the check box next to each server that you want to include in the report, then from the **Resource** menu choose **Export to CSV**.

Chapter 5: Exploring Servers and Groups in SAS Client

IN THIS CHAPTER

This section discusses the following topics:

- Device Explorer
- Device Explorer Interface
- Server Information
- Device Groups
- Device Group Explorer

Device Explorer

The Device Explorer feature of the Opware SAS Client allows you to browse and manage servers, devices, and groups of servers in your environment. Using the Device Explorer you can perform the following actions on individual servers:

- Browse Opware information such as properties, configurable applications, and server history.
- Browse the file system, registry, hardware inventory, software and patch lists, and services.
- View virtual servers, either hypervisors or VMware VMs and Solaris local zones.
- Drag-and-drop files between your desktop and servers.
- Perform an audit of the server or view where the server is being used in an audit.
- Take a snapshot of the server.
- View packages and patches installed on the server.
- View group membership for the server (what device groups the server belongs to).
- Configure applications on the server.

- Manage software policies.
- Add and delete custom attributes.
- View summary and history information.

You can also browse groups of servers and perform the following operations for groups of servers:

- Browse groups of servers and access servers inside of groups, including physical and virtual servers
- Perform an audit of servers in the group.
- Take a snapshot of servers in the group.
- View software and patch policies associated with the group of servers.

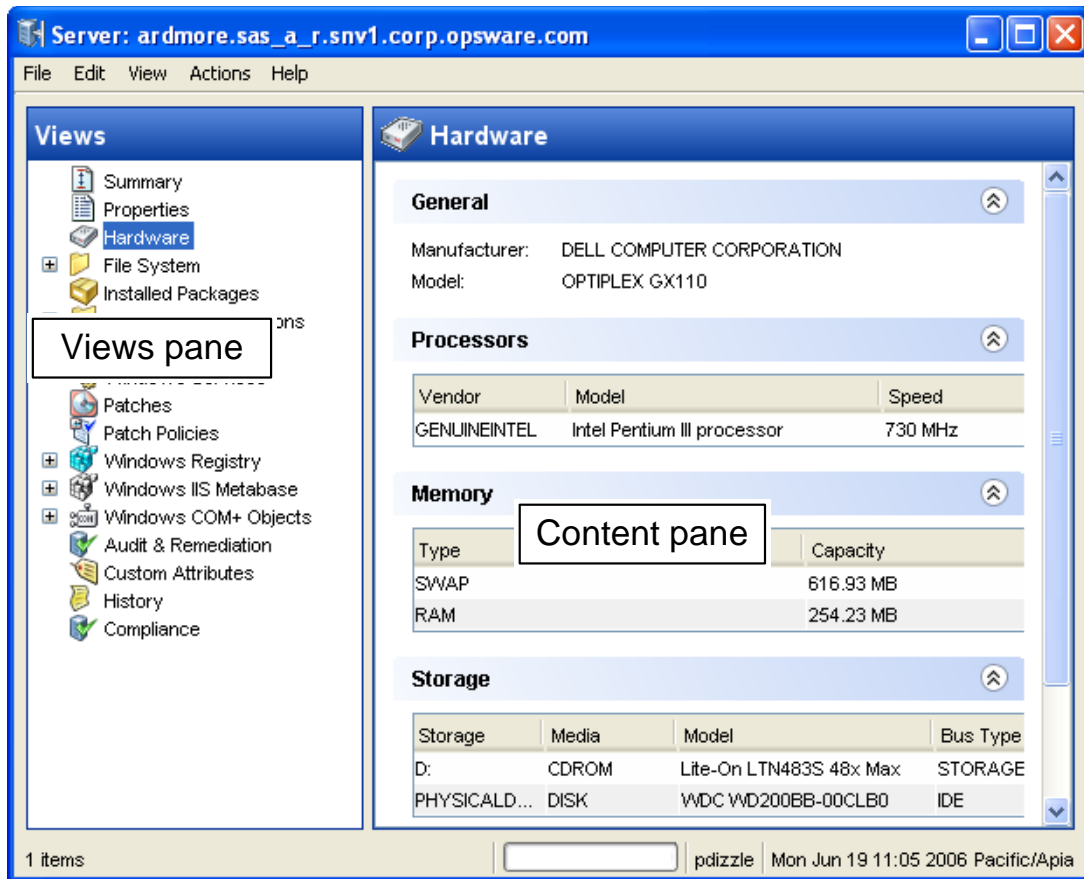


When you perform an action on a group of servers, the action applies to all members of the group, including sub groups and their members. However, changes applied to an Application Configuration at the group level only apply to members of the group, but do not apply to sub groups of the parent group.

Device Explorer Interface

The Device Explorer consists of two main components: the Views pane and the Content pane. The Views pane lists server objects from the managed server, and the Content pane displays content for each of the server's objects. When you select a server object in the Views pane, its corresponding content appears in the Content pane. See Figure 5-1.


Figure 5-1: Device Explorer Interface



Accessing the Device Explorer

To access the Device Explorer, perform the following steps:

- 1** Launch the SAS Client and then from the Navigation pane, select **Devices** ► **All Managed Servers**.
- 2** A list of servers will display in the Content pane.

If the list of servers is long, use the search tool  to locate a server (upper right corner) by name, IP address, OS, customer, facility, or description. If you search by user name, the text entry is case insensitive.

You can also sort the list by clicking a column heading, such as name, IP address, OS, customer, and so on. To reverse sort, click the column heading a second time.

- 3** Open a server from the Contents pane. This opens the Device Explorer. From the **Actions** menu, you can perform the following operations:
 - View more detailed information about the selected server in the SAS Web Client.
 - Access the Visual Application Manager.
 - Audit or configure application configurations.
 - Perform an audit.
 - Create a snapshot.
 - Create a package.
 - Attach a software policy.
 - Install a patch, export patch information to .csv.
 - Run a compliance scan.
 - Add or delete custom attributes.
 - Open a remote terminal.

Action menu items change according to the server object selected.

For example, if you select the Configured Applications object from the server object tree, then from the **Actions** menu, you can add a configuration, remove a configuration, create a package, and so on.

Opening a Remote Terminal

You can open a remote terminal for any managed server, but not a group of servers. To do so, perform the following steps:

- 1** Launch the SAS Client. From the Navigation pane, select **Devices** ► **All Managed Servers**.
- 2** Select a managed server and open it.
- 1** In the Device Explorer window, from the **Actions** menu, select **Launch Remote Terminal**.

2 Log into the remote terminal.

See “Opening a Remote Terminal” on page 398 in Chapter 10 for more information.

Server Information

The Device Explorer allows you to review the following server information:

- Summary
- Properties
- Hardware
- File System
- Configured Applications
- Software Policies
- Services
- Patches
- Patch Policies - Windows Only
- Windows Registry
- Windows IIS Metabase
- Windows COM+ Objects
- Audit and Remediation
- Custom Attributes
- Group Membership
- Server History
- Compliance
- Virtualization

Summary

The Summary view lists the following information:

- **System:** This displays operating system information.
- **Manufacturer:** This displays server manufacturer, hardware, and system details.

- **Opsware Registration:** This displays communication status, when the server was last registered, how many applications and patches are registered with Opsware SAS, and so on.

Properties

The Properties view lists the following property information for the server that you are browsing:

Management Information

- **Name:** This displays the name of the managed server.
- **Notes:** This displays any notes listed.
- **IP Address:** This displays the IP address of the managed server.
- **OS Version:** This displays the operating system (platform) that the managed server is running on.
- **Customer:** This displays an account within Opsware SAS that has access to designated resources, such as servers and software.
- **Facility:** This displays the location of the server. Users can manage servers in any facility from an SAS Web Client.
- **Realm (link speed):** This displays the minimum bandwidth limit between the Opsware Agent and the core (if the agent is going through gateways).
- **Server Use:** This displays how an organization is using the managed server; for example, a server could be a staging server, a production server, a development server, and so on.
- **Deployment Stage:** This displays the stages of deployment for a server; for example, a server could be live or offline.
- **Opsware Lifecycle:** This displays the server's stage in the Opsware Lifecycle; for example, unprovisioned, available, managed, or deactivated.
- **Server ID:** This displays the internal ID that Opsware SAS uses to identify the server.
- **Status:** This displays whether or not the server is reachable and thus managed by Opsware SAS. "OK" means that the server (its Opsware agent) is reachable; unreachable means that there is a communication problem and Opsware SAS cannot communicate with the server.

Reported Information

- **Reporting:** This displays information about the ability of the server's agent to communicate with the core. Statuses include Has not reported, OK, Registration in progress, and Reporting error.
- **Agent Version:** This displays the version number of the agent.
- **Hostname:** This displays the hostname of the managed server.
- **Reported OS:** This displays the operating system (platform) that the managed server is running on.
- **MAC Address:** This displays the Media Access Control (MAC) address. This is the network interface card's unique hardware number. The MAC address is used as the server's physical address on the network.
- **Serial Number:** This displays the serial number of the system. Opware SAS attempts to report a chassis ID if possible.
- **Chassis ID:** This displays a unique hardware-based identifier that the Opware Agent discovers, typically derived from some property of the server's chassis. As a common source for this ID, Opware SAS uses an interface's MAC address or the host ID on Solaris servers, or the serial number for one of the interfaces.
- **Encoding:** This displays the character encoding of the managed server, such as Shift_JIS (Japanese) or Windows 1252 (Western).

From this window, you can also open a remote terminal on the selected server.

Hardware

The Hardware view lists all the reported hardware on the selected managed server. This includes the following information:

- **Processors:** This lists the processor information for all processors on the managed server.
- **Memory:** This lists the total amount and the types of memory on the managed server.
- **Storage:** This lists all storage devices on the managed server.
- **Network Interfaces:** This lists the network interfaces on the managed server.

File System

The File System view enables you to browse the file system of a managed server. The File System has two main sections (similar to the Windows file system explorer): the server's directories and the contents of the selected directory.

The left side navigation panel of the Device Explorer shows all the directories of the selected server, and the right side of the Device Explorer lists the contents of the selected directory.

For each file, the SAS Client lists the file's name, size, type, and date modified. To sort the files by any of these categories, click on the top of the column.



Depending upon your user permissions, you might not have access to a particular server's file system. In such a case, you cannot select and view the server's file system in the Device Explorer. If you have access to a server's file system, then you will see user names, such as Administrator, root, and Local System. These are user names used to access that server's file system as the selected user.

Viewing File Contents

To view file contents, perform the following steps:

- 1** Launch the SAS Client. From the Navigation pane, select **Devices ► All Managed Servers**.
- 2** A list of servers will display in the Content pane. Select a server and open it. This opens the Device Explorer.
- 3** From the left side of the Device Explorer, select a File System object.
- 4** You are prompted to select a user name to log into the computer, such as Administrator, LocalSystem, or root. Select a user.
- 5** To view the contents of disk drives or folders, expand the icon. Select a directory.
- 6** From the **Actions** Menu, select **View Contents**. The file content view pane appears at the bottom of the window.
- 7** To change the character encoding, select an item from the Encoding drop-down list.

Ways to Copy Files

You can copy files from a server to another directory on the same server, to a directory on another Opsware-managed server, or to your local computer (where the SAS Client is running). You can also copy a file from your local computer to a directory on the managed server. A few restrictions apply when copying files on a managed server's file system using the Device Explorer:

- You cannot copy folders/directories.
- You can only copy to servers that you have permissions to write to and to view.
- You can only copy one file at a time.
- You cannot undo a deletion – once you delete a file, it's gone.

Copying Files Between Managed Servers

To copy files between managed servers, perform the following steps:

- 1** Launch the SAS Client. From the Navigation pane, select the **Devices ► All Managed Servers**.
- 2** To launch the Device Explorer, open a server from the server list.
- 3** From the left side of the Device Explorer, select a File System object. To view the contents of disk drives or folders, expand the icon.
- 4** Navigate to the directory that contains the file that you want to copy and select it.
- 5** From the **Actions** Menu, select **Copy To**.
- 6** In the Copy To dialog box, select from the following locations in the drop-down list:
 - Managed Servers (other managed servers in the core)
 - This Server
 - Local File System
- 7** Navigate to the desired directory.
- 8** Click **Select**.

Copying Files from Your Computer to a Managed Server

To copy files from your computer to a managed server, perform the following steps:

- 1** Launch the SAS Client. From the Navigation pane, select **Devices ► All Managed Servers**.

- 2 To launch the Device Explorer, open a server from the server list.
- 3 From the left side of the Device Explorer, select a File System object.
- 4 Navigate to the target directory where you want to copy the file.
- 5 Use your system's file system explorer to select the file that you want to copy, then drag the file to the desired location in the Device Explorer.

Deleting Files

Once you delete a file, it cannot be recovered. (However, before you delete, you are prompted with a confirmation dialog box.)

To delete a file, perform the following steps:

- 1 Launch the SAS Client. From the Navigation pane, select the **Devices ► All Managed Servers**.
- 2 To launch the Device Explorer, open a server from the server list.
- 3 From the left side of the Device Explorer, select a File System object.
- 4 Select a file to delete from the Content pane.
- 5 From the **Actions** menu, select **Delete**.
- 6 Click **Yes** in the confirmation dialog box.

Renaming Files

To rename a file, perform the following steps:

- 1 Launch the SAS Client. From the Navigation pane, select the **Devices ► All Managed Servers**.
- 2 To launch the Device Explorer, open a server from the server list.
- 3 From the left side of the Device Explorer, select the File System object. To view the contents of a folder, expand the folder.
- 4 Select the file that you want to rename, and from the **Actions** menu, select **Rename**.
- 5 Enter a new name for the file, then press ENTER. Pressing the ESC key on your keyboard will cancel the rename operation.

Creating a Configuration Template from a File

For any file on a managed server, you can create an Application Configuration Template.

To create an Application Configuration Template from a file, select the file. From the **Actions** Menu, select **Create Configuration Template**. See *Opsware[®] SAS User's Guide: Application Automation* for more information.

Creating a Package from a File

For any file on a managed server, you can create an installable software package. For each package, you can specify the customer assignment, the reboot requirements, and the pre/post install and pre/post uninstall scripts.

To create a package from a file on the managed server file system, select the file. From the **Actions** Menu, select **Create Package**. See *Opsware[®] SAS Policy Setter's Guide* on how to create a package.

Installed Packages

The Installed Packages view enables you to view any installed packages on the selected managed server. For each package, you can view name, type, size, last modified, and description. To sort the list by these categories, click the title of each column. See the *Opsware[®] SAS Policy Setter's Guide* on how to create a package.

Configured Applications

The Application Configurations view in the Device Explorer gives you access to application configurations and configuration templates, and shows you configuration files on the selected managed server being managed by Opsware.

Installed Configurations

In the Content pane, the Installed Configurations tab of the Configured Applications window allows you to browse and edit all Application Configurations attached to the managed server.

In the Views pane, expand the Configured Application icon to display all applications being managed by the Application Configuration Management System. (If you cannot expand the Application Configurations folder, then no Application Configurations have been attached to the server.)

Each application can contain one or more instances of a managed application on the server. You can expand each application to view and edit values sets for each managed application. For more information about setting values for an Application Configuration, see the *Opsware[®] SAS User's Guide: Application Automation*.

Configuration History

The Backup Configurations tab of the Configured Applications window provides a history of all changes made to the selected application configuration template, and allows you to revert to a previous version of the configuration. Thus, you can rollback the current state of an application configuration to any previous state in this list.

To rollback the configuration to a previous state, select an item in the list and click **Revert**.

Software Policies

The Software Policies view displays all software policies associated with the selected server (or group of servers).

Show Options

You can use the Show drop-down list to filter the following types of software policies:

- **Policies Attached Servers:** This displays all policies attached to the server, or policies attached to a group of servers to which the selected managed server belongs.
- **Non-Compliant Policies:** This displays the software policies attached to the selected server which are non-compliant with the actual server configuration.
- **Policies which Require Scan:** This displays the software policies for which the software compliance information is not yet calculated.
- **Policies Currently Scanning:** This displays the software policies for which software compliance information is being calculated.

From the **Actions** menu, you can perform actions such as attaching a policy, detaching a policy, remediating a server, and scanning software compliance.

Services

The Services window shows you a list of all running services on the selected managed server. Depending on the installed operating system, you can perform different operations on the services:

- For Windows services, you can start, stop, pause, resume, and restart a service. You can also set the service to start manually, to start automatically when the system is rebooted, or to be disabled altogether.
- For Linux servers (supported by Red Hat and SuSE versions), you can perform any action that a particular service supports. Supported actions may vary from service to

service, for example, start, stop, restart, condrestart, or status. You can also specify the run levels that you want a service to run under.

To perform an operation on a service, select the service and right-click.

Patches

This window displays all patches associated with the selected managed server.

Show Options - Windows

You can use the Show drop-down list to filter the following types of patch information:

- **Patches Installed:** This option displays all patches that have been installed on the server.
- **Patches Recommended By Vendor:** This option displays all application and operating system patches that have been recommended by Microsoft (MBSA 2.0) for the selected server. If multiple patches have the same QNumber, Patch Management detects the application files that are already installed on a managed server and, subsequently, recommends the correct patch to install.
- **Patches with Policies or Exceptions:** This option displays patches in policies attached to the selected server, or patches that have always install exceptions, *and* have one of the following conditions:
 - The patches are not currently installed and are recommended by the vendor.
 - The patches are currently installed.
- **Patches Needed:** This option displays all patches that should be installed on the selected server but are not. These include patches that are in policies attached to that server, or patches that have always install exceptions, *and* are recommended by the vendor.
- **Patches with Exceptions:** This option displays all patches that have exceptions (such as always install or never install) *and* have one of the following conditions:
 - The patches are not currently installed and are recommended by the vendor.
 - The patches are currently installed.
- **All Patches:** This option displays all patches that are associated with the operating system of the server.

Show Options - UNIX

The Show options for UNIX patches display the following information:

- **All Patches:** This option displays all patches that are associated with the operating system of the server.
- **Patches Installed:** This option displays all patches that have been installed on the server.

Patch Contents – Windows

The Show options for Windows patches display the following information:

- **Icon:** A dimmed icon means that the patch has not yet been uploaded to the Software Library.
- **Name:** This is the QNumber of a patch that is a hotfix or an update rollup. Service pack patches do not have a QNumber.
- **Compliance:** This shows one of the following three levels of patch compliance, as defined by a patch administrator:
 - **Non-Compliant** (red): This indicates that the patch is installed on the server, but is not in the policy, or that the patch is not installed on the server but is in the policy.
 - **Partial** (yellow): This indicates that the policy and exception do not agree, and the exception does not have data in the Reason field.
 - **Compliant** (green): This indicates one of the following conditions:
 - A patch is installed on the server and is in a policy, or a patch is not installed on the server and is not in a policy.
 - A patch is installed on the server and there are additional patches with the same QNumber in a patch policy or exception. In this case, all patches with the same QNumber are considered installed when Patch Management calculates patch compliance.
 - A patch is not installed on the server and is in a patch policy or has an always install exception, and is not recommended by the vendor. In this case, the patch has a never install exception, because it is not recommended by the vendor.

In the Preview pane, move the cursor over the icon or text in the Compliance column to view patch compliance information about a server.

- **Type:** This shows the type of patch, such as Windows Hotfix or Windows Update Rollup.

- **Bulletin:** (Optional) This shows the Microsoft Security Bulletin ID number for this patch.
- **Severity:** (Optional) This shows one of the following three Microsoft severity ratings for this patch:
 - **Critical:** This indicates a patch whose exploitation could allow the propagation of an internet worm, without user action.
 - **Important:** This indicates a patch whose exploitation could result in a compromise of the confidentiality, integrity, availability of user data, or of the integrity or availability of processing resources.
 - **Moderate:** This indicates a patch whose exploitability is mitigated to a significant degree by certain factors, such as default configuration, auditing, or the difficulty of exploitation.
 - **Low:** This indicates a patch whose exploitation is extremely difficult, or whose impact is minimal.
- **Release Date:** This displays the date that Microsoft released this patch.
- **Exception:** This displays the type of patch policy exception set for the selected server.
- **Installed:** This shows if the patch is installed on the selected server.
- **Recommended:** A check mark indicates that this patch was recommended by the vendor (MBSA 2.0) during the last software registration.
- **Description:** This displays a description of the server.
- **Opware ID:** (Optional) This displays a unique Opware ID that identifies the patch object.
- **Locale:** (Optional) This displays the encoding of the patch contents.
- **OS:** (Optional) This displays the operating system version of the server.

Patch Contents – UNIX

This shows the following Unix patch content information:

- **Icon:** A dimmed icon means that the patch has not yet been uploaded to the Software Library.
- **Type:** This shows the type of patch, such as Solaris Patch, HP-UX Patch Fileset, and so on.
- **Installed:** This shows if the patch is installed on the selected server.

- **Description:** This displays a description of the server.
- **Install Date:** This displays the date the patch was installed on the server.
- **Opware ID:** (Optional) This displays the unique Opware ID that identifies the patch object.
- **OS:** (Optional) This displays the operating system version of the server.

Patch Policies - Windows Only

This window displays all patch policies associated with the selected Windows managed server (or server group).

Show Options

The Show drop-down list displays the following patch policy information:

- **Policies Attached to the Server:** This displays all policies attached to the Windows server, or policies attached to a server group to which the selected Windows managed server belongs.
- **Policies Not Attached to the Server:** This displays a list of all patch policies relevant to the selected server that are not attached to the server.

Patch Contents

This section displays the following patch policy content information:

- **Name:** This displays the name of the patch policy.
- **OS:** This displays the operating system associated with the patch policy.
- **Description:** This shows a description of the patch policy.

Windows Registry

This window displays a read-only view of the Windows registry on the selected Windows managed server. You can navigate to this registry much like the regedit tool on the Windows operating system.

Folders on the left side of the window represent keys in the registry. Clicking a folder on the left displays entries in a key in the right window.

To view Windows Registry items, select the top-level Windows Registry icon in the Server Explorer and select a user from the menu. Your user must have proper permissions to view Windows Registry keys. If your user is unable to access the Windows Registry for the selected managed server, contact your Opsware administrator.



The HKEY_CLASSES_ROOT might have thousands of entries and can take time to load.

Windows IIS Metabase

This window displays a read-only view of the IIS Metabase on the selected Windows managed server. You can browse the IIS Metabase much like one of the metabase browsing tools such as metaedit or the IIS Metabase Browser.

The left side of the Metabase window displays the hierarchical layout of the metabase tree. Selecting an item in the tree on the left shows the data items associated with the selected key in the right hand view. Clicking the (+) symbol to the left of a key item will expand the item's child keys.

To view Windows IIS Metabase items, select the top-level Windows Metabase icon in the Server Explorer, right-click, and select a user. Your user must have permissions to view Windows Metabase items. If your user is unable to access the Windows Registry, contact your Opsware administrator.

Windows COM+ Objects

This window displays a read-only view of all the COM+ objects on the selected managed server. In the Server Explorer window, the Views pane displays the following two folders for browsing COM+ objects:

- **All Objects:** This is a flat list of all the COM+ objects on the managed server.
- **Component Categories:** This contains an alphabetical list of all COM component categories.

To view the contents of a COM+ object, perform the following steps:

- 1** Select the All Objects or the Component Categories folder. In the Content pane, expand the folder until you reach an object.
- 2** To view the contents of a COM+ object, from the Actions **Menu**, select **View Contents**. The contents will then display.

- 3** If the content of the COM+ object uses a different encoding, choose the appropriate encoding type from the Encoding drop-down list.

You must have specific user permissions to view Windows COM+ objects. If you are unable to access the Windows Registry, contact your Opsware administrator.

Audit and Remediation


The Audit and Remediation view shows the following information for the selected server:



- **Audit - Server is Source:** Shows all audits where the selected server is used as the source of the audit.
- **Audit - Server is Target:** Shows all audits where the selected server is the target of the audit.
- **Audit Results - Server is Source:** Shows the results of all audits where the selected server was used as the source of the audit.
- **Audit Results - Server is Target:** Shows the results of all audits where the selected server was used as the target of the audit.
- **Snapshot - Specifications:** Shows all snapshot specifications that are using this server as one of its targets.
- **Snapshots:** Shows all snapshot results that used this server as a target.

Custom Attributes

This window displays the custom attributes set to a server or group of servers. You can add, edit or remove custom attributes from this window.


Custom attributes can be one of the following two types:

- Inherited  from another source, such as a customer, a software policy, group of servers, ISM control, and so on.
- Attached directly to the server.

To override inherited custom attribute values, click the inherited arrow icon  once, and enter a new value in the value field. Press ENTER. The inherited arrow changes  to indicate that the custom attribute value has been overridden.

Group Membership

The group membership view displays all the device groups that the server belongs to.

If the list of servers is long, use the search tool  to locate a server (upper right corner) by name, description, access, location, or type. If you search by user name, the text entry is case insensitive.

You can also sort the list by clicking a column heading, such as name, description, access, location, or type. To reverse sort, click the column heading a second time.

For more information on device groups, see “Group Membership” on page 158.

Server History

The Server History view shows changes made to the selected server. For example, it displays who modified a server, what change was made, when it was modified, and so on. Server history specifically shows when a user has performed one of the following actions:

- Added the server to a node
- Removed the server from a node
- Reassigned the server from one node to another

Entries are generated when actions are performed for managed servers in the SAS Web Client. The History is read-only. Each entry shows the following information:

- **Event:** A description of the change.
- **Date:** The date when the last change occurred.
- **User:** The user who made the change.

Use the View drop-down list to sort the server history list according to a range of time, such as last week, the last two months, and so on.

Compliance

The Compliance view of the Device Explorer displays the compliance levels for the selected server and allows you to determine if your server is in compliance with the following categories:

- **Software:** Software compliance indicates whether or not all software policies attached to the selected server are compliant with the actual server configuration. A software policy includes installed packages and patches, application configurations, and other software policies. If the actual server configuration does not match the software policy definitions, then the server's software policies are considered out of compliance.

- **App Config:** An Application Configuration defines how specific application configurations files should be configured on a managed server. Application Configuration compliance indicates whether or not all of the Application Configurations attached to a server are compliant with the actual application configuration files on the server. If the actual server configuration does not match the Application Configuration definitions, then the server's Application Configurations are out of compliance.
- **Patch:** Patch Compliance determines whether all patches in a patch policy and a patch policy exception were installed successfully. To test patch compliance, servers are scanned to determine whether they conform to their attached policies and exceptions, based on compliance status and rules. If any of the patches defined in the patch policy do not match what is actually installed on the server, then the server's patch policies are out of compliance.
- **Audit:** The Compliance Dashboard displays these two types of compliance for audits:
 - All roll up of scheduled audits will appear by default in the Compliance Dashboard in a single column named audit. This status enables you to view the total compliance status of all audits scheduled to run on a regular basis on the selected server. A server at any given time can be the target for several audits. This compliance test provides a roll up of compliance status for all audits being run against the server.
 - Individual audits that have been scheduled to run on the selected server can be displayed on a per-audit basis. These audits will not appear by default and must be activated to be displayed in the Compliance Dashboard. In order to view an individual audit for a specific server in the Compliance Dashboard, you must have access to view that server where the audit is running.

Virtualization

The Virtualization view displays information about virtual servers – both hypervisors and virtual guest servers. For example, for a hypervisor server, the Virtualization view displays all virtual servers being hosted on the server. For virtual servers, the Virtualization views displays all virtual server information as well as the hypervisor server name that is hosting it.

Solaris 10 – Device Explorer

You can use the Device Explorer to view a Solaris 10 global zone hypervisor and local zone server information. A global zone or local zone as seen through the Device Explorer looks nearly the same as a regular physical server, except it has an extra property named “Virtualization,” which provides the following information:

- **Hypervisors:** When you view a Solaris 10 global zone hypervisor in the Device Explorer, the Virtualization view shows all hosted local zones. From here you can also stop and start the local zones.
- **Solaris Local Zones:** When you view a Solaris local zone in the Device Explorer, the Virtualization view indicates the name of its hypervisor, its reserved CPU shares, and virtual hardware information.

VMware ESX 3 – Device Explorer

You can use the Device Explorer to view a VMware ESX VM or a hypervisor's server information. A VM as seen through the Device Explorer looks nearly the same as a regular physical server, except it has an extra property named "Virtualization," which provides the following information:

- **Hypervisors:** When you view a VMware ESX hypervisor in the Device Explorer, you can see all of its hosted VMs.
- **VMware ESX VMs:** When you view a VMware ESX VM in the Device Explorer, the Virtualization view shows you the VM's virtual server properties, its virtual network configuration, and its data store configuration.

Device Groups



This section contains information about managing device groups in the SAS Client. See "Server Groups" on page 280 in Chapter 8 for information about managing groups in the SAS Web Client.

The Device Groups feature provides a useful way for gathering servers into collections or organize groups of servers. Grouping servers enables you to perform the same action such as installing patches, remediating servers on all of the servers simultaneously, instead of performing the action on individual servers, one at a time.

Device groups can consist of individual servers as well as other device groups.

In Opware SAS, some of the recommended ways of grouping servers include:

- Grouping servers by OS version
- Grouping servers by customer

- Grouping servers by facility
- Grouping servers by deployment stage
- Grouping servers by use
- Group servers by virtual technology
- Grouping servers by operational boundaries, for example, grouping together all servers that require identical application configuration
- Grouping servers to control access, for example, creating device groups that are associated with a specific user group

A device group acts as a container for a collection of servers. Operations that can be performed on a server can be performed on a device group. As a result a device group enables you to perform an action on multiple servers and avoid repeating the same operation on each individual server. When any of the operations, such as installing software or patch and configuring application configurations, are performed on a device group, they are actually performed on the servers within the group, and not on the group itself.

Characteristics of Device Groups

Device groups have the following characteristics:

- Individual servers can be included in many device groups or not included in any device groups.
- Adding servers to a device group does not remove those servers from the list of all servers that appear in the All Managed Servers list in the SAS Client.
- Device groups can contain servers and other device groups.
- Device groups are hierarchical (they can be nested) with the following caveats:
 - Private and public groups cannot be mixed in a hierarchy, but static and dynamic groups can.

See "Types of Device Groups" on page 163 in this chapter for more information about private and public groups.

- The rules for a dynamic group are not inherited from a parent dynamic group to a dynamic subgroup.

See "Dynamic Device Groups" on page 164 in this chapter for more information about the characteristics of dynamic groups.

- Groups do not inherit custom attributes from their parents.
- When you run an operation on a group that contains nested groups, the operation also applies to all the servers in the nested groups below the current group.
- When an Application Configuration operation within the SAS Client is applied to groups, and those groups contain subgroups, the operation does not apply to all the servers in the subgroups. It only applies to the group upon which the operation was directly applied.

Types of Device Groups

There are two types of device groups, private groups and public groups, and each can be either static or dynamic.

Public and Private Device Groups

Public Device Groups

Public device groups can be created, edited, or deleted by any user who has Manage Public Device Groups permissions. Public groups are visible to all users, and can be used by any Opware user. Only users with Manage Public Device Group permission can add members to a static public device group or change the rules that govern the dynamic public device group. Public device groups can also be used for modeling.

Accessing servers in a public device groups also depends on the Device Group permission in the SAS Web Client. See *Opware[®] SAS Administration Guide* for more information about setting device group permissions.

Public Device Group Modeling

With Opware modeling, the desired state of a server is defined and then applied to servers. In the case of public device groups (static and dynamic), you can define a model consisting of application configurations, patch policies, software policies, and custom attributes, which will be applied to all servers in the group. The modeling information is attached to the group, but not to any subgroups.

If the modeling information changes, the servers in the group are not affected until the remediate operation runs on those servers. If the model has already been remediated on that server when it is removed from the group, the installed material will be removed during the next remediation.

Private Device Groups

Private device groups can be created by any user belonging to a user group that has access to the Manage Servers list. Only the user who creates the private device groups can see and manage them. These groups are not visible to the other Opware users. Private groups behave the same way as public groups, with the exception that modeling is not available for private groups. See “Public Device Groups” on page 163 in this chapter for more information.

Static and Dynamic Device Groups

Static Device Groups

A static group has servers that are added to and removed from the group manually. When using static groups, you first create the group, and then select the servers to populate it. Static groups can be either public or private, and no specific permissions are required for creating static groups.

Dynamic Device Groups

Dynamic device groups contain servers that are added to or removed from the group based on a set of user-defined rules. If the rules are changed or the servers in the environment change, servers will be added to or removed from the group automatically. Rules apply only to the group being created or modified and not to any of the subgroups.

Once the rules have been created, Opware SAS will search for servers that match the criteria of that specific group, and add them to the group. When the rules are changed, Opware SAS will search again, and the resulting group members reflect the changed criteria. Consequently, as servers are added to or removed from management using Opware SAS, the members of the group will change automatically.

Opware SAS calculates server group membership each time any of the following actions occur:

- After users add, delete, or change the rules for dynamic device groups.
- When attributes of servers change such that dynamic group membership could change.

Additionally, Opware SAS automatically recalculates dynamic group membership every hour.

Ways to Create Device Groups

In the SAS Client, you can create a device group from the Manage Servers list or by performing a server search, and saving the resulting list of servers or the rules as a group.

Creating a Static Device Group

Static device groups require servers to be added to them manually. The servers in a static group also must be removed manually.

A static group without servers added can be converted to a dynamic group. Conversely, a static group that has servers cannot be converted to a dynamic group.



To create a public static device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

To create a static device group, perform the following steps:

- 1** From the navigation pane, select **Devices** ► **Device Groups**. The list of device groups appears in the Content pane.
- 2** To create a public static device group, select public group and then from the **Actions** menu, select **New** ► **Static Group**.

Or

To create a private static device group, select private group and then from the **Actions menu**, select **New** ► **Static Group**.

The name of the device group that you just created is New Device Group (n), where n is a number based on the number of new device groups already in existence.

- 3** Enter the name of the device group in the Content pane
- 4** Press the Enter key to save the device group.



To create a device group in a specific location, navigate to the desired location in the device group hierarchy and then select **New** from the **Actions** menu.

After you create a static device group, you can add servers to that group. See “Adding a Server to a Static Device Group” on page 169 in this chapter for more information.

Creating a Dynamic Device Group

Dynamic device groups are rule-based, and the servers in dynamic groups will be added or removed automatically based on the rules defined by you.

When a dynamic device group is converted to a static device group, all the servers remain in the static device group, but the rules used to define the server membership are lost.



To create a public dynamic device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

To create a dynamic group, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The list of device groups appears in the Content pane.
- 2** To create a public dynamic device group, select public group and then from the **Actions** menu, select **New** ► **Dynamic Group**.

Or

To create a private dynamic device group, select private group and then from the **Actions** menu, select **New** ► **Dynamic Group**.

The name of the device group that you just created is New Device Group (n), where n is a number based on the number of new device groups already in existence.

- 3** Enter the name of the device group in the Content pane.
- 4** Press the Enter key to save the device group.



To create a device group in a specific location, navigate to the desired location in the device group hierarchy and then select **New** from the **Actions** menu.




After you create a dynamic device group, you can define the rules for the group. See “Adding a Server to a Dynamic Device Group” on page 171 in this chapter for more information.

Creating a Device Group Groups Using Search



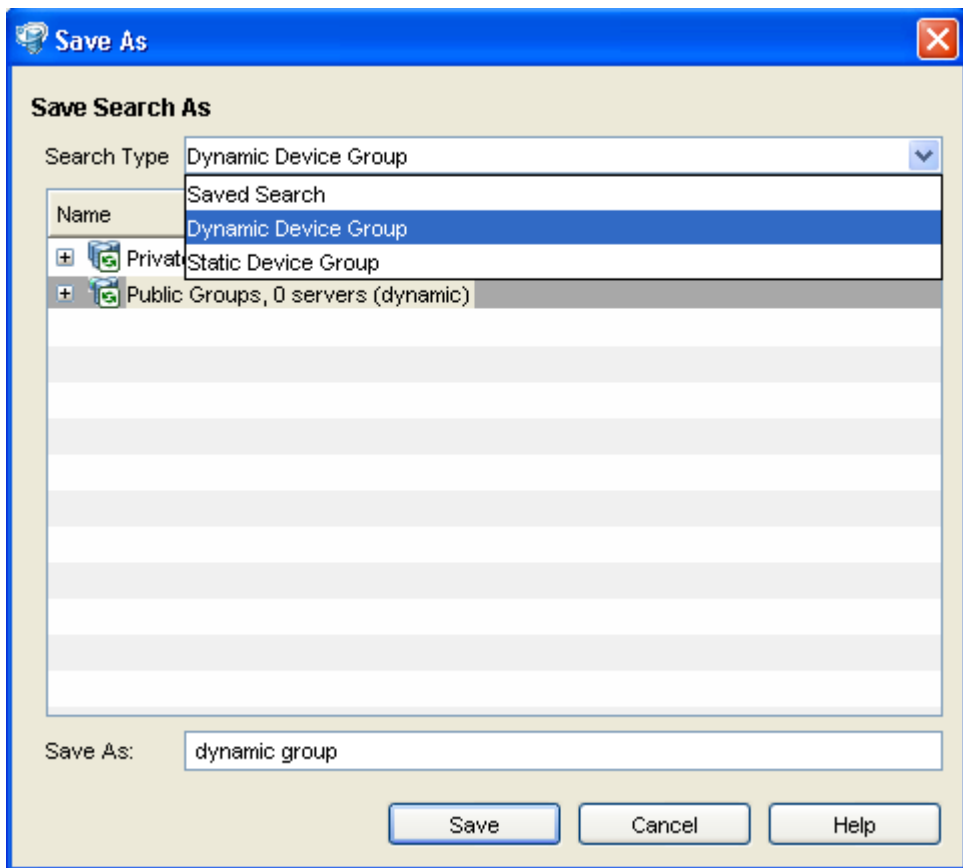
To create a public device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

To create a device group using search, perform the following steps:

- 1** From the Navigation pane, select **Search**.
- 2** Click **Advanced Search**. The Advanced Search page appears in the Content pane.
- 3** From the first drop-down list, select Server.
- 4** Create a rule by selecting the attribute from the second drop-down list. Depending on the attribute that you select, options available for the operator and values for the rule will change.
- 5** Select the operator from the third drop-down list. The operator selected defines how the search text is treated.
- 6** Enter a value in the field or select a value from the drop-down list or click  to select multiple values from the **Select Values** window.
- 7** Click  to add additional rules and repeat steps 4 to 6. Click  to delete any rules.
- 8** Select the logic (And/Or) to be applied for every rule in the query.
- 9** Click **Search** to run the search query. The search results appear in the Content pane.

- 10** Click **Save** to save your search query. The Save Search window appears as shown in the figure below. In the Search Type drop-down list, select Dynamic Device Group or Static Device Group. Specify the location and then enter the name of the device group in the Save As text box and click **Save**. The name of the saved search cannot be more than 64 characters.

Figure 5-2: The Save Search Window in the SAS Client



When you save the device group as a dynamic group, if the rules change or the servers in the environment change, servers will be added to or removed from the device group automatically. When you save the device group as a static group, the servers will be added to the device group, but all rules will be lost.



If the search query does not return any results, then you can only save the device group as a dynamic device group.

Adding a Server to a Static Device Group



To add a server to a public static device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opware Administrator.

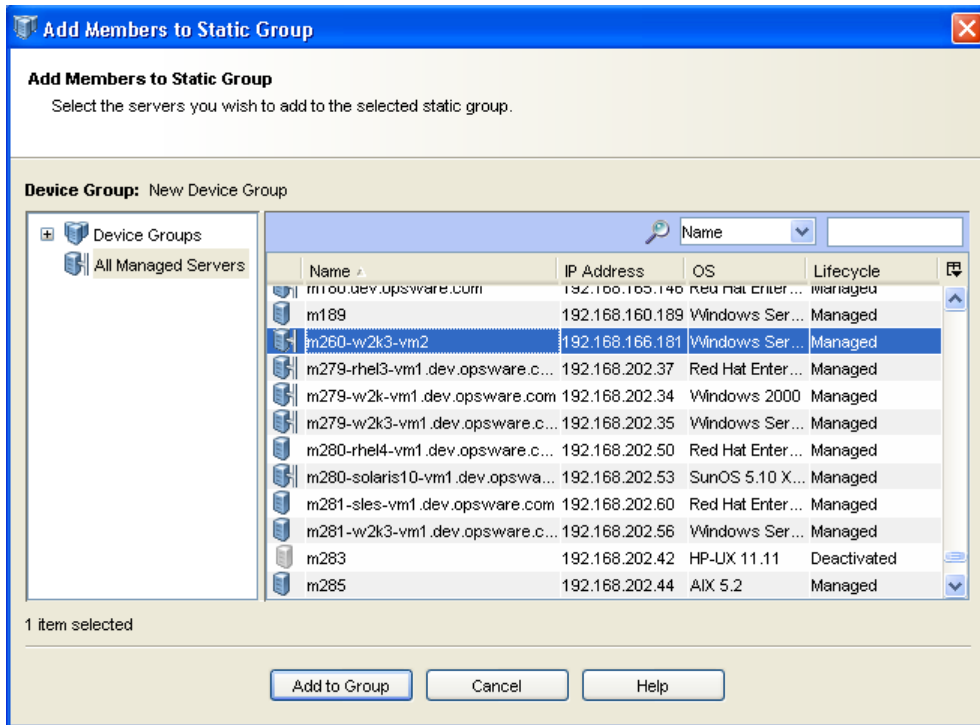
Method 1

To add a server or device group to a static device group, perform the following steps :

- 1** From the Navigation pane, select **Devices** ► **Device Group**. The device groups appear in the Content pane.
- 2** Select a static device group and from the **Actions** menu, select **Open**. The Device Group Explorer appears.
- 3** From the Views pane, select Server Membership.

- 4 From the **Actions** menu, select **Add Members**. The Add Members to Static Group window appears.

Figure 5-3: The Add Members to Static Group Window in the SAS Client



- 5 Select the servers or device groups to add to the static device group.
- 6 Click **Add to Group**. The selected servers or device groups appear in the Device Group Browser.
- 7 From the **File** menu, select **Save** to save the device group.

Method II

Perform the following steps to add a server to a static device group:

- 1 From the Navigation pane, select **Devices** ► **All Managed Servers**. The list of managed servers appears in the Content pane.
- 2 From the Content pane, select the servers and then from the **Actions** menu select **Add to Device Group**. The Add to Group window appears.
- 3 Select the static device group to add the servers and then select **Add to Group**. The selected servers are added to the static device group.

Adding a Server to a Dynamic Device Group

Servers are added to dynamic device groups automatically, based on the rules created for the group. You can change the membership of a dynamic group by adding, deleting, or updating the dynamic group rules.



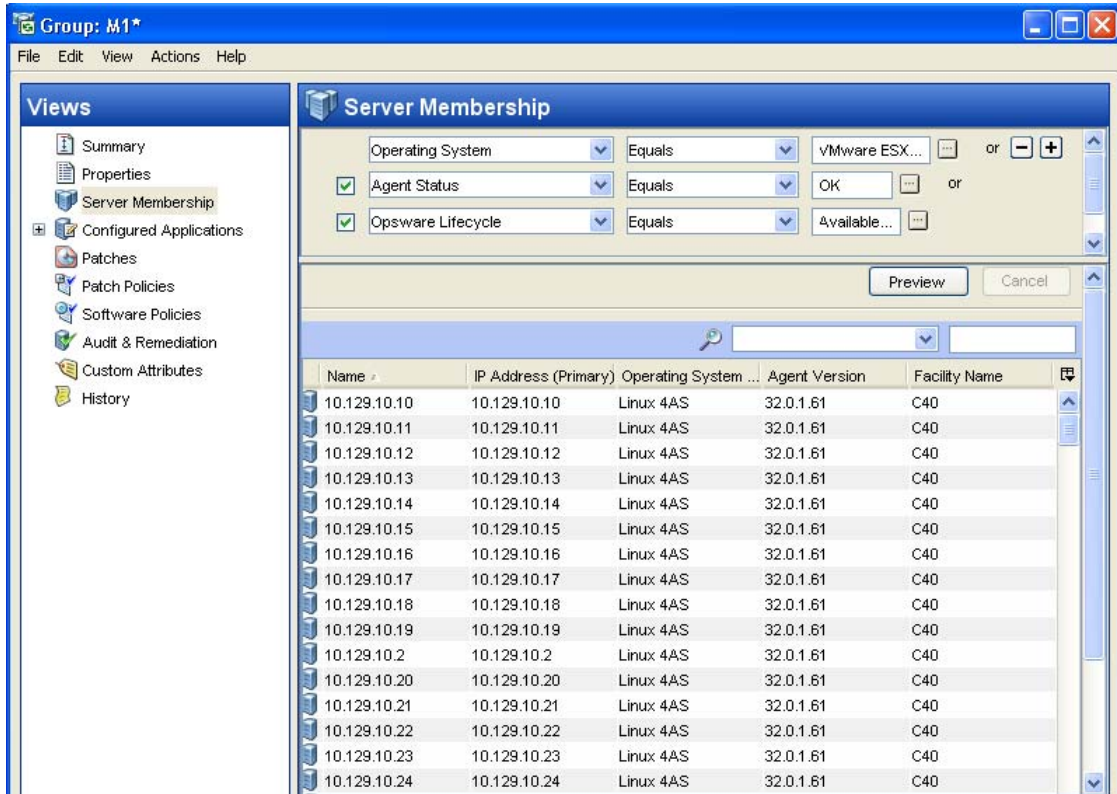
To add a server to a dynamic public device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opware Administrator.




To add a server to a dynamic group, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The list of device groups appear in the Content pane.
- 2** From the Content pane, select the device group and then from the **Actions** menu, select **Open**. The Device Group Explorer appears.

- 3 From the Views pane, select Server Membership. In the Content pane, you can specify the rules for the dynamic device group. See Figure 5-4.

Figure 5-4: Defining Rules for a Dynamic Device Group



- 4 Create a rule by selecting the attribute from the first drop-down list. Depending on the attribute that you select, options available for the operator and values for the rule will change.
- 5 Select the operator from the second drop-down list.
- 6 Enter a value in the field, or select a value from the drop-down list, or click  to select multiple values from the Select Values window.
- 7 Click  to add additional rules and repeat steps 4 to 6. Click  to delete any rules.
- 8 Select the logic (And/Or) to be applied for every rule in the query.
- 9 Click **Preview** to view the servers which are members of the device group.

- 10** From the **File** menu, click save to **Save** the rules.

Removing Servers from a Static Device Groups

In a static device group, servers have to be removed manually. Removing a server only removes the server from the device group and not from the Manage Server list. Servers can belong to more than one device group, so if you want to remove a server from each device group that it belongs to, then you must locate and remove each instance of the server from all the device groups.



To remove servers from a public device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

Method I

To remove a server from a static device group, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The list of device groups appears in the Content pane.
- 2** Select a static device group and from the **Actions** menu, select **Open**. The Device Group Explorer appears.
- 3** From the Views pane, select Server Membership. The list of servers and device groups in the device group appear in the Content pane.
- 4** Select the server or device group. From the **Actions** menu, select **Remove Members**. The server or device group selected is removed from the static device group.

Method II

To remove a server from a static device group, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The Device groups appear in the Content pane.
- 2** Select the device group and double click to display its members.
- 3** Select the server displayed in the Content pane. From the **Actions** menu select **Remove Members**. The server selected is removed from the static device group.




Removing Servers from a Dynamic Group

Servers are added or removed from dynamic device groups automatically, based on the rules created for the group. To remove servers, you can update the rules. These rules apply only to the group being created or modified, and not to any of the subgroups.



To remove servers from a public dynamic device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opware Administrator.

To update the rules for a dynamic device group, perform the following steps :

- 1** From the Navigation pane select **Devices ► Device Groups**. The list of device groups appear in the Content pane.
- 2** From the Content pane, select the device group and then from the **Actions** menu, select **Open**. The Device Group Explorer appears.
- 3** From the Views pane, select Server Membership. In the Content pane, you can specify the rules for the dynamic device group.
- 4** Update a rule by selecting the attribute from the first drop-down list. Depending on the attribute that you select, options available for the operator and values for the rule will change.
- 5** Select the operator from the second drop-down list.
- 6** Enter a value in the field or select a value from the drop-down list or click  to select multiple values from the Select Values window.
- 7** Click  to update additional rules and repeat steps 4 to 6. Click  to delete any rules.
- 8** Select the logic (And/Or) to be applied for every rule in the query.
- 9** Click **Preview** to view the servers which are members of the device group.
- 10** From the **File** menu, click **Save** to save the rules.

Moving a Device Group

Moving a device group moves the location of the device group to the desired location. In the SAS Client, you can move device groups from a private group to a public group. You cannot move device groups from a public group to a private group. If you move a device group containing sub groups the sub group are also moved to the desired location.



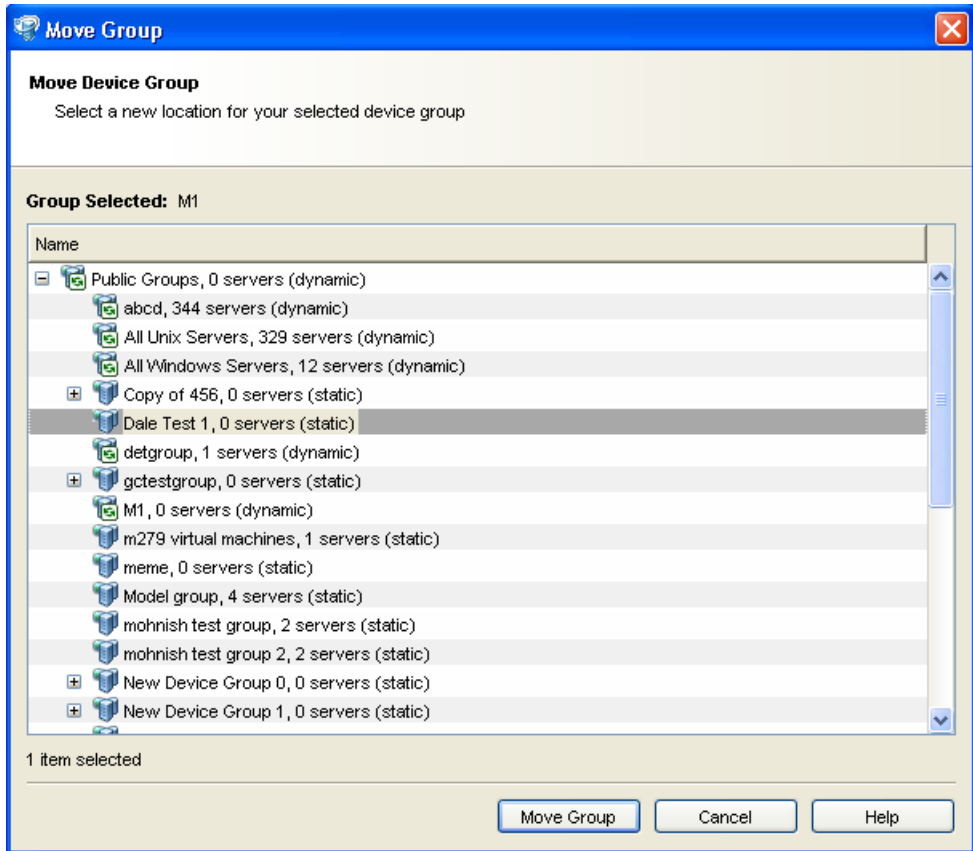
To move a public device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

To move device groups from one group to another, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The list of device groups appears in the Content pane.

- From the Content pane, select the device group and then from the **Actions** menu, select **Move Group**. The Move Device Group window appears as shown below.

Figure 5-5: The Move Device Group Window in the SAS Client



- Select the desired location to move the device group.
- Click **Move to Group**. The device groups are moved to their new location.

Duplicating a Device Group

When you duplicate a device group the servers are copied to a new group and they remain in the original group. In the SAS Client, you can only select one device group at a time to duplicate.



To duplicate a public device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

To duplicate an existing device group, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The list of device groups appears in the Content pane.
- 2** From the Content pane, select a device group and then from the **Actions** menu, select **Duplicate Group**. A copy of the device group is created.

Deleting a Device Group

Deleting a device group removes the group, but the servers in the group still remain in the Manage Servers list and in any other groups for which they are members.

A group cannot be deleted when any of the following conditions apply:

- Software policies or patch polices are attached to the group or a subgroup of the group.
- Access control boundaries are attached to the groups or a subgroup of the group.
- The device group contains servers and other device groups.



To delete a device group, you require Manage Public Device Group permission. To obtain these permissions, contact your Opsware Administrator.

To delete a server group, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The list of device groups appears in the Content pane.
- 2** From the Content pane, select the device group and then from the **Actions** menu, select **Delete Group**.
- 3** Click **Delete** on the confirmation dialog to delete the device group.

Device Group Explorer

The Device Group Explorer allows you to view and manage the properties of a device group in the SAS Client. From the Device Groups Explorer, you can perform the following actions:

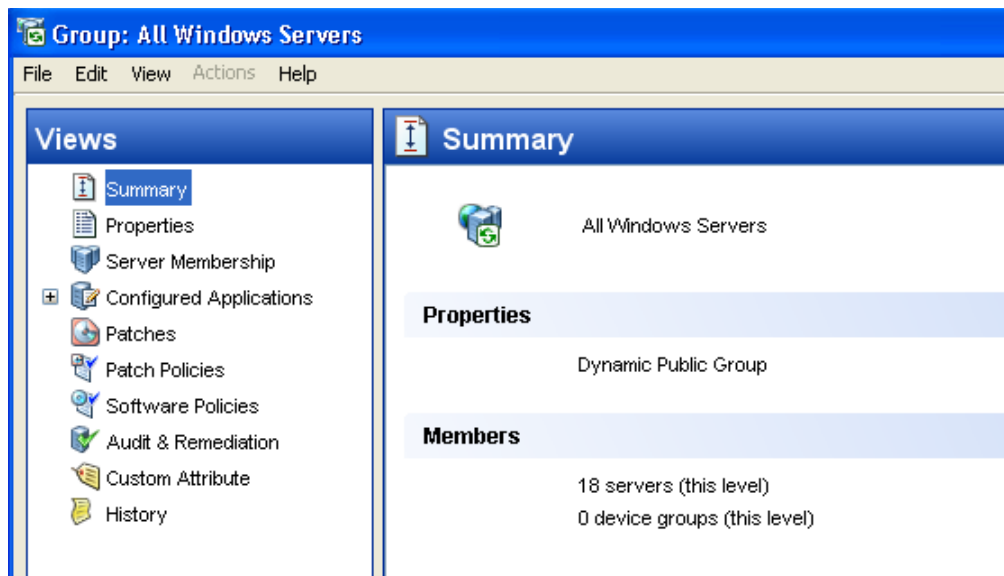
- View the properties and members of a device group.
- Change a dynamic device group to a static device group.
- Add or remove members from a device group.
- Add application configurations to a device group.
- View and manage patches, patch policies and software policies associated with the servers in the group.
- Create an audit.
- Take a snapshot.
- View and create custom attributes.
- View server history.

See “Device Group Explorer” on page 179 in this chapter for more information.

To access a Device Group Explorer, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**. The Device groups appear in the Content pane.
- 2** Select a device group and from the **Actions** menu select **Open**. The Device Group browser appears as shown below.

Figure 5-6: The Device Group Explorer Window



- 3** Select the various views in the Views pane to view the properties or perform any actions on the device group.
 - **Summary:** This window allows you to view the type of device group and the members associated with the device group.
 - **Properties:** This window allows you to view the properties of the device group and edit the Name, Description, and the Type of the device group.
 - **Server Membership:** This window allows you to view the members associated with the device group and also manage members in the device group.
 - **Configured Applications:** This window allows you to view and edit application configurations attached to a device group, and add an application configuration to the device group.
 - **Patches:** This window allows you to view all the patches associated with the device group, add patches to a patch policy, and install patches on the device group.
 - **Patch Policies:** This window allows you to view all the patch policies associated with the device group, and remediate the servers in the device group with the patch policies.
 - **Software Policies:** This window allows you to view all the software policies associated with the device group and remediate the servers in the device group with the software policies.
 - **Audit and Remediation:** This window allows you to create and run audits and snapshots.
 - **Custom Attributes:** This window displays the custom attributes set to a device group and allows you to add, edit or remove custom attributes from a device group.
 - **History:** This window allows you to view the changes made to a device group. For each action on the group (but not group members), the history displays the date, the action occurred, and the user who performed the action (if the group is public).

Device Group Explorer

The Device Groups Explorer provides access to all groups of servers and other devices in the core. From the Device Groups Browser, you can perform the following actions:

- Browse groups of servers and access servers inside of groups:

- View patches, patch policies and software policies associated with the servers in the group.
- Create an audit.
- Take a snapshot.
- View and create custom attributes.
- View server history.

Accessing the Device Groups Explorer

To access the Device Groups Explorer, perform the following steps:

- 1** Launch the SAS Client and select **Devices ► Device Groups**.
- 2** Select a device group and open it. (You can expand a group to find sub groups.)
- 3** If the list of device groups is long, sort the list by clicking a column name, such as name, IP address, OS, customer, or facility.
- 4** For each device group, you can also perform an audit, take a snapshot, or configure applications.

Device Group Explorer Interface

The Device Group Explorer allows you to review the following information about a group of servers:

- Summary
- Properties
- Server Membership
- Configured Applications for Device Groups
- Patches for Device Groups
- Patches for Device Groups
- Software Policies for Device Groups
- Audit and Remediation
- Custom Attributes for Device Groups
- History Properties for Device Groups

Summary

The Summary view lists the following information:

- **Properties:** This displays if the device group is Private, Public, Dynamic or Static.
- **Members:** This displays the total number of members in the device group.

Properties

The Properties view lists the following property information such as name, type, status, accessibility for the group of servers that you are browsing.

Server Membership

From inside each device group, you can view all members – managed servers and other groups of servers and other devices – that belong to the group. For each server that belongs to the group, the system displays its name, IP address, OS, customer, facility, and any description.

Configured Applications for Device Groups

If the device group is public, then you can add an Application Configuration to the group. The Application Configuration applies to all servers and groups in this group.

- The Installed Configurations tab allows you to browse and edit all Application Configurations attached to the device group.
- The Backup Configurations tab provides a history of all changes made to the selected application configuration template, and allows you to revert to a previous version of the configuration.

See *Opware[®] SAS User's Guide: Application Automation* for more information.

Patches for Device Groups

This window displays all patches associated with the selected server group.

Show Options

You can use the Show drop-down list to filter the following types of patch information displayed in the Device Groups Explorer.

- **Patches with Exceptions (Windows Only):** This option displays all patches that have exceptions for Windows servers (such as always install or never install) *and* have one of the following conditions:
 - The patches are not currently installed and are recommended by the vendor.

- The patches are currently installed.
- **All Patches:** This displays all patches that are associated with the operating system of a server.

Patch Contents

This section displays the following patch contents information.

- **Icon:** This displays a dimmed patch icon when the patch has not yet been uploaded to the Software Library.
- **Name:** This indicates the QNumber of a patch that is a hotfix or an update rollup. Service pack patches do not have a QNumber.
- **Compliance:** This shows one of the following three levels of patch compliance, as defined by a patch administrator:
 - **Non-compliant** (red): This indicates that the patch is installed on the server, but that it is not in the policy, or the patch is not installed on the server but is in the policy.
 - **Partial** (yellow): This indicates that the policy and exception do not agree, and that the exception does not have data in the Reason field.
 - **Compliant** (green): This indicates any of the following conditions:
 - A patch is installed on the server and is in a policy, or a patch is not installed on the server and is not in a policy.
 - A patch is installed on the server and there are additional patches with the same QNumber in a patch policy or exception. In this case, all patches with the same QNumber are considered installed when Patch Management calculates patch compliance.
 - A patch is not installed on the server and is in a patch policy or has an always install exception, and is not recommended by the vendor. In this case, the patch has a never install exception because it is not recommended by the vendor.

In the Preview pane, move the cursor over the icon or text in the Compliance column to view patch compliance information about a server.

- **Type:** This indicates the type of patch, such as Windows Hotfix or Windows Update Rollup.
- **Bulletin:** (Optional) This indicates the Microsoft Security Bulletin ID number for this patch.

- **Severity:** (Optional) This displays one of following Microsoft severity ratings for this patch:
 - **Critical:** This indicates a patch whose exploitation could allow the propagation of an internet worm, without user action.
 - **Important:** This indicates a patch whose exploitation could result in a compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources.
 - **Moderate:** This indicates a patch whose exploitability is mitigated to a significant degree by factors, such as default configuration, auditing, or difficulty of exploitation.
 - **Low:** This indicates a patch whose exploitation is extremely difficult, or whose impact is minimal.
- **Release Date:** This shows the date that Microsoft released this patch.
- **Exception:** This indicates the type of patch policy exception set for the selected server.
- **Installed:** This indicates if the patch is installed on the selected server.
- **Recommended:** A check mark indicates that this patch was recommended by the vendor (MBSA 2.0) during the last software registration.
- **Description:** This shows a description of the server.

Patch Policies for Device Groups

This window displays all patch policies associated with the selected device group. You can use the Show drop-down list to filter the type of patch policies to display in the Server Explorer.

Show Options

This section displays the following patch information:

- **Policies Attached to Device Group:** This displays all policies attached to the device group, or policies attached to a server group to which the selected managed server belongs.
- **Policies Not Attached to the Server:** This displays a list of all patch policies relevant to the selected server group that are not attached to the group.

Patch Contents

This section displays the following patch content information:

- **Name:** This displays the name of the patch policy.

- **OS:** This displays the operating system associated with the patch policy.
- **Description:** This shows a description of the patch policy.

Software Policies for Device Groups

This Software Policies view displays all software policies associated with the selected server (or group of servers). You can perform actions such as attaching a policy, detaching a policy, remediating a server, and scanning software compliance from the **Actions** menu.


Audit and Remediation



This window allows you to create and run audits and snapshots.

Custom Attributes for Device Groups

This window displays the custom attributes set to a server or device group. You also can add, edit or remove custom attributes from this window.

Custom attributes can be one of the following two types:

- Inherited  from another source, such as a customer, a software policy, group of servers, ISM control, and so on.
- Attached directly to the server.

To override inherited custom attribute values, click the inherited arrow icon  once, and enter a new value in the value field. Press ENTER. The inherited arrow changes  to indicate that the custom attribute value has been overridden.

History Properties for Device Groups

The History view shows changes made to the selected device group. Entries are generated when actions are performed on a device group in the SAS Web Client. The History is read-only. Each entry shows the following information:

- **Date:** The date when the last change occurred.
- **Event:** A description of the change.
- **User:** The user who made the change.

Use the View drop-down list to sort the device group history list according to a range of time, such as last week, the last two months, and so on.

Chapter 6: Virtualization Director

IN THIS CHAPTER

This section discusses the following topics:

- Virtualization Director Overview
- Key Terms and Concepts
- Virtualization Director Permissions
- Virtualization Director Usage
- Viewing Virtual Servers in the SAS Client
- Virtual Servers in VAM
- Virtual Servers in the SAS Web Client
- Virtual Server Status
- Solaris Local Zone Management
- Searching for Virtual Servers
- Creating Device Groups for Virtual Servers

Virtualization Director Overview

The Opsware Virtualization Director feature enables you to provision and manage virtual servers for Solaris 10 local zones and VMware ESX 3 virtual machines (VMs). Using the SAS Client, you can perform the following tasks:

- View both hypervisor and virtual servers and their relationships in the SAS Client, so you can find out the hypervisors that are hosting your virtual machines and local zones.
For more information, see “Viewing Virtual Servers in the SAS Client” on page 194.
- View virtual servers and their relationship in the Visual Application Manager (VAM).
For more information, see Chapter 7, “Visual Application Manager” on page 59 of this guide.

- Provision VMware ESX and Solaris 10 hypervisors on bare metal servers.

For more information on setting up a bare metal server to be provisioned with either VMware ESX 3 or Solaris 10, see Chapter 15, "Operating System Provisioning".

- Provision VMware virtual machines (VM) using an OS sequence. For example, once you have provisioned a VMware ESX hypervisor you can then provision a new VM as an individual bare metal server using the Opware OS Provisioning feature.

For more information on setting up an OS installation profile, see "Creating an OS Installation Profile" on page 21.

For more information on setting up and running an OS sequence, see "Creating an OS Sequence" on page 22.

- Create, start, stop, modify, and remove Solaris local zones.

For more information, see "Solaris Local Zone Management" on page 213.

- Deploy agents on unmanaged virtual servers using the Opware Agent Discovery and Deployment (ODAD) for VMware ESX VMs.

For more information on deploying agents on unmanaged servers, see Chapter 4, "Opware Agent Management".

- Report on managed virtual servers.

For more information, see "View Virtual Server in Reports" on page 202.

- Search for virtual servers in your data center using the Search tool.

For more information on searching for virtual servers, see "Searching for Virtual Servers" on page 225.

- Create dynamic Device Groups based upon virtual server characteristics (zones or VMs).

For more information, see "Creating Device Groups for Virtual Servers" on page 228.

Virtualization Director Permissions

Like all features in Opware SAS, the Virtualization Director feature is governed by permissions. To obtain these permissions, contact your Opware administrator and see the *Opware® SAS Administration Guide*.

Key Terms and Concepts

While there are many different virtual server technologies on the marketplace today, the underlying concept of virtual server technology is basically the same across most platforms: a single, physical server is configured to run as a hypervisor “host” to one or more virtual servers, or “guests.”

The following terms are used to discuss virtual server technologies by Opware SAS, Solaris 10, and VMware ESX:

- **Hypervisor:** The host operating system for virtual servers.
 - **Global Zone:** The term Solaris 10 uses for the hypervisor server, upon which local zones (complete OS instances) are installed and hosted.
 - **VMware ESX Server:** The term VMware ESX uses for the hypervisor server.
- **Virtual Server:** A logical server that appears to an operating system and application as a traditional server, but which is actually an emulated environment on top of a traditional server. For example, Solaris 10 and VMware ESX use the following terminology to refer to virtual servers:
 - **Local Zone:** The term Solaris uses for a virtual server. More technically speaking, a zone is a complete OS instance hosted on a Solaris global zone hypervisor. (Sun sometimes also refers to local zones as “containers,” but in this document we use the term “local zone.”)
 - **Virtual Machine** The term VMware ESX uses to refer to a virtual server.

Virtualization Director Usage

The Virtualization Director reaches across many features in Opware SAS, allowing you to manage your virtual servers in many ways, as illustrated by the following examples:

- OS Provisioning Virtual Servers – Overview
- Solaris 10 Local Zone Management Usage Examples
- Search and Group Virtual Servers
- Report on Virtual Technologies
- View Virtual Servers in VAM

OS Provisioning Virtual Servers – Overview

You can use the OS provisioning feature to provision a server with an operating system that supports virtualization technologies (VMware ESX 3 and Solaris 10) and then you can use the Virtualization Director in the SAS Client to manage the virtual servers that run on them.

The main difference for servers provisioned with hypervisor operating systems is that you can create new virtual servers on a hypervisor server outside of Opware SAS. This means that those virtual servers created outside of Opware SAS will appear in the SAS Client as unmanaged servers, and they will need to have an Opware Agent installed on them to be managed by the Opware system.

This process works differently between VMware ESX 3 and Solaris 10:

- **VMWare ESX:** Since Opware SAS 6.1 does *not* support creating VMs, you will need to use the VMWare console to create your VMs. Then, you can use the OS Provisioning and Opware Agent Discovery and Deployment (ODAD) features to bring the new VMs under Opware SAS management.
- **Solaris 10:** Since Opware SAS 6.1 *does* support the creation of local zones, you can use the OS Provisioning and Virtualization Director features to provision Solaris 10 and create new local zones. You can also use Opware Agent Discovery and Deployment (ODAD) to install Opware Agents on local zones created outside of Opware SAS.

You can use ODAD to provision VMWare ESX and Solaris 10 hypervisors and the virtual servers that run on them – and install an Opware Agent when necessary. The following sections illustrate this:

- Provision VMware ESX Hypervisor and VMs
- Provision Solaris 10 Hypervisor and Install Agents on Local Zones



For more information on setting up a bare metal server to be provisioned with either VMware ESX 3 or Solaris 10, see Chapter 15, “Operating System Provisioning”.

Provision VMware ESX Hypervisor and VMs

You can use the Opsware SAS OS Provisioning feature to provision the VMware ESX 3 operating system on a bare metal server, which works much like provisioning on the Linux operating system. For information about setting up OS provisioning for VMware ESX 3, see the *Opsware® SAS Policy Setter's Guide*.

After the VMware ESX 3 hypervisor server has been provisioned, the SAS Client recognizes this server and displays it in both the All Managed Servers and Virtual Servers list. It is then manageable by Opsware SAS.

Using the VMware console, you can create new virtual servers (VMs) and install full operating systems on them. (You can see any new VMs by using the Refresh hypervisor function.) In order to bring those new VMs under Opsware SAS management, they will need Opsware Agents installed on them. You can deploy Opsware Agents on the new VMs using the Opsware Agent Discovery and Deployment (ODAD).

For information on using ODAD, see Chapter 4, "Opsware Agent Management".

Using the VMware console, you can also create new VMs that do *not* have an operating system on them, and instead use the OS Provisioning feature to provision the new VMs with new operating systems. You can boot these new "bare metal" VMs into the SAS Web Client server pool using the VMware console (either using PXE boot or boot image files). When you launch the SAS Client, you can also view these same unprovisioned VMs in the Unprovisioned Servers list.

Using the OS Provisioning feature in the SAS Client, you can select an OS sequence that contains the OS you want to provision onto the VM just like you would for a regular physical server, and then provision the new VM with the chosen operating system. (These could be three different VMware ESX 3 supported operating systems, such as Windows XP, Red Hat Linux, and so on.)

Once these new VMs have been provisioned, they appear to the SAS Client just like a regular managed server and can be configured for compliance, have patches installed on them, be viewed in VAM, have their application configurations managed, and so on.



For more information on setting up an OS installation profile, see "Creating an OS Installation Profile" on page 21. For more information on setting up and running an OS sequence, see "Creating an OS Sequence" on page 22.

Provision Solaris 10 Hypervisor and Install Agents on Local Zones

You can use the OS Provisioning feature to install Solaris 10 on a bare metal server, then once that server appears in the SAS Client as a managed server, you can create local zones using the Virtualization Director feature.

For example, you can provision a bare metal server with the Solaris 10 operating system, and once it has finished installing the OS, the server appears in the SAS Client in the Virtual Servers list. Then, you can select the Solaris 10 server, right-click, and create a new local zone on that server. This new local zone now functions as any other managed server in the SAS Client, and can be audited, patched, visualized in VAM, logged into with a remote terminal, and so on.

After a Solaris 10 server has been provisioned, it is possible that someone will create new local zones on it outside of the SAS Client. You can see the new local zones by using the Refresh hypervisor function. To bring these new local zones under Opware management, you need to install agents on the new local zones.

In the Virtual Servers list, you can view the Solaris 10 hypervisor and install Opware Agents on the new local zones. This is done by selecting an unmanaged local zone from the Virtual Server list, right-clicking, and choosing to install the Opware Agent. This local zone now functions as any other managed server in the SAS Client.

For more information on working with Solaris zones, see "Solaris Local Zone Management" on page 213.

Solaris 10 Local Zone Management Usage Examples

The Virtualization Director enables you to perform the following Solaris 10 local zone management tasks:

- Create a Local Zone
- Install an Opware Agent on a Local Zone
- Stop and Start a Local Zone
- Modify a Local Zone
- Remove a Local Zone

Create a Local Zone

Once a systems engineer or an administrator has provisioned a server with the Solaris 10 operating system and it has been set up to support zones, you can view the new Solaris 10 hypervisor (global zone) in the Virtual Servers list inside the SAS Client. (See “View Virtual Server Relationships” on page 194.) From here, you can select the hypervisor, right-click, and use the Create Zone window to create a new local zone.

For more information on creating a local zone, see “Creating a Local Zone” on page 214.

Install an Opware Agent on a Local Zone

It is possible to create a new local zone on a Solaris 10 hypervisor that is being managed by Opware SAS. These new zones will be visible inside of the SAS Client, but in order to manage them and perform operations on them (such as performing an audit, installing patches, tracking compliance, and so on), you need to install an Opware Agent on the local zone.

Before you install an Opware Agent on a local zone created outside of Opware, make sure that all the services are up and running in the local zone.

For more information, see “Installing an Opware Agent on Unmanaged Solaris Local Zone” on page 212.

Stop and Start a Local Zone

If you manage local zones on Solaris 10 servers, you might get a work order to stop five specific local zones on a hypervisor. This may be because the applications running on five of those local zones are going to be upgraded and cannot be used during that time. In such a case, you can use the SAS Client to stop a local zone in order to free up system resources on the hypervisor. When the applications on the five stopped zones are upgraded, you can log into the SAS Client, select each zone, and start them back up.

For more information, see “Starting and Stopping Local Zones” on page 213.

Modify a Local Zone

The original amount of CPU shares allocated for a zone might need to be increased, for a number of reasons. For example, you could receive a work order to increase the CPU share of a zone if it was discovered that an HTTP server running on the local zone was performing sluggishly due to increased usage. If initially, the CPU shares allocated for the zone are set to one, then you can stop the zone, and using the Modify Virtual Zone window, increase the CPU share allocation to four.

For more information on modifying an existing local zone, see “Modify a Local Zone” on page 191.

Remove a Local Zone

When a zone is no longer needed or the application that is running on it is no longer needed or has been deprecated, you can easily remove the local zone to free up system resources on the hypervisor.

For more information on deleting a local zone, see “Removing a Local Zone” on page 223.

Search and Group Virtual Servers

You can search for virtual servers in your data center based upon several criteria, and once you find them, add those virtual servers into a dynamic Device Group. The dynamic Device Group allows you to configure criteria that define the group's membership and filter out any servers that do not meet that criteria.

For example, you might be responsible for patching VMs running Windows XP Pro. You can do a search using the SAS Client search tool and find all VMs running Windows XP Pro. Once you get the results, you can group those servers in the search results into a dynamic Device Group, and then build rules that define the membership of the group according to that criteria. For example, if you search for all solaris local zones that have CPU shares under 5, you can create a similar filter for the dynamic Device Group, so you can be sure that the group will always only contain local zones that meet that criteria. Then, you can perform operations on the group, such as launching the Software Management feature to Remediate patches on the servers in the group.

For more information, see “Searching for Virtual Servers” on page 225 or see “Creating Device Groups for Virtual Servers” on page 228.

Report on Virtual Technologies

Reporting on virtual servers can help you understand not only how many servers in your data center are virtual (and what virtual technology they are running), but specifically which servers in the data center are virtual as opposed to those which are not.

It also helps you see which servers are hypervisors and which are virtual servers, and helps ensure that a hypervisor does not fail and potentially affect all the virtual servers that it is hosting.

For example, you can get a clear picture of how much of your data center is running virtual servers, what number of these virtual servers are running Solaris 10, and which are running ESX 3. Lastly, you might want to see a list of all virtual servers in relation to their hypervisors.

You can open the SAS Client, and from the Navigation pane, select the Virtual Servers folder, and select the following reports:

- **All Virtual Servers:** Shows all managed virtual servers (hypervisors and virtual servers).
- **Virtual Servers by Virtualization Technology:** Shows all virtual servers by vendor.
- **Virtual Servers by Hypervisor:** Shows all virtual servers grouped by hypervisor (Solaris Global Zones and VMware ESX hypervisors).
- **Resource Allocation by Hypervisor:** Shows resource allocation by hypervisor (Solaris Global Zones and VMware ESX hypervisors).

For more information, see “View Virtual Server in Reports” on page 202.

View Virtual Servers in VAM

VAM gives you an in-depth understanding of the applications that run on virtual servers. You can open the Opsware SAS Client, select a virtual server that you know the application runs on, and launch VAM.

VAM scans the selected server and discovers all applications, component signatures, processes and process families, and connections related to all the applications on the selected servers. VAM displays detailed “maps” of the application (processes and process families) and servers and connections associated with the servers selected (virtual and non-virtual), as well as any related network relationships.

Viewing the Virtual Map, you can click on the server to expand it, see all application processes running on it, and gain valuable visibility into the hypervisor on which the VM runs.

Viewing Virtual Servers in the SAS Client

You can view virtual servers from several different perspectives inside the SAS Client. The following sections illustrate this:

- View Virtual Server Relationships
- View Virtual Servers in All Managed Servers List
- View Virtual Servers in the Device Explorer
- View Virtual Server in Reports

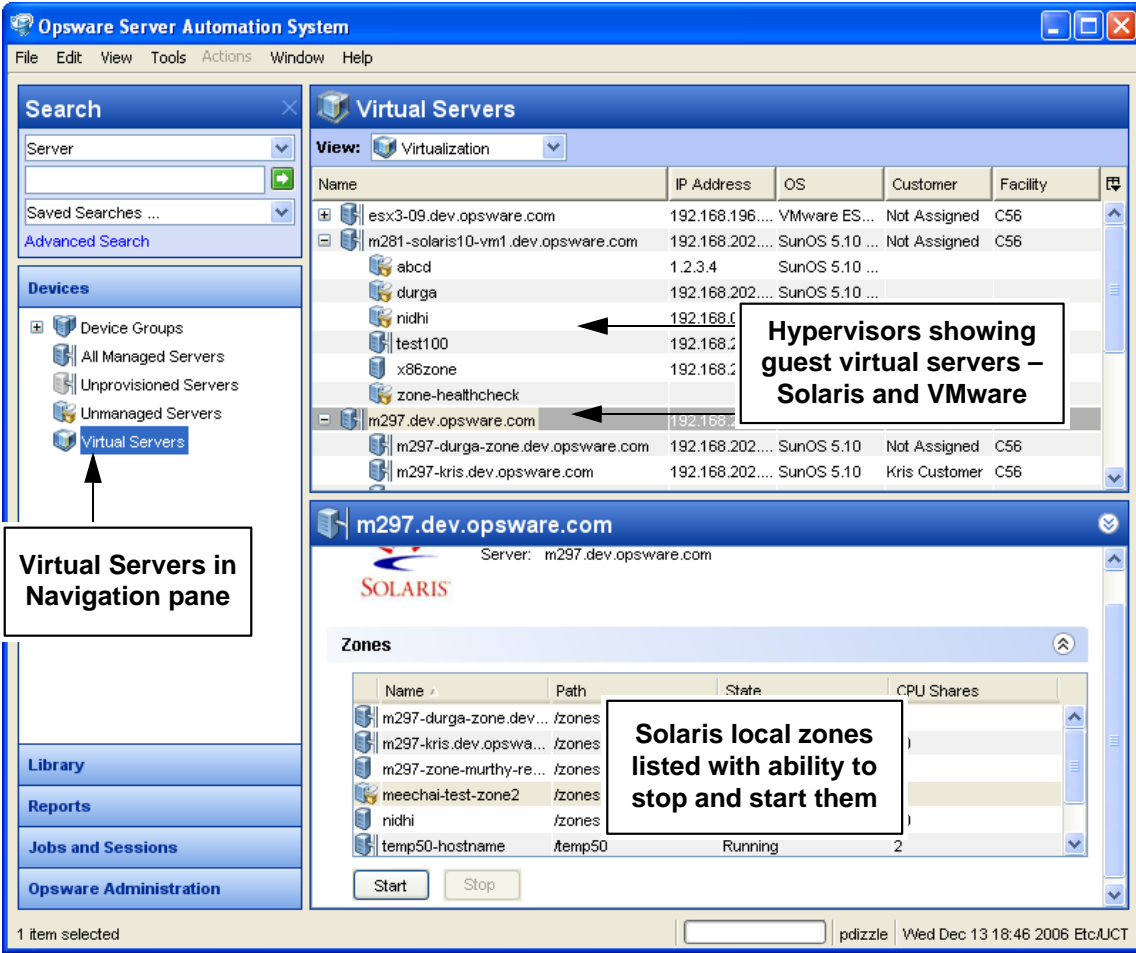
View Virtual Server Relationships

In the SAS Client, you can view all of your managed virtual servers and their relationships to their hypervisors by selecting Virtual Servers in the Navigation pane, as shown in Figure 6-1.



You can view hypervisors and virtual servers from multiple virtualization technologies in a single user interface in the SAS Client.

Figure 6-1: SAS Client Showing Virtual Servers Relationships



Viewing virtual servers in the SAS Client allows you to view virtual server relationships to their hypervisors, and perform all the other basic server management operations just as you do on a regular physical server.

For Solaris 10 local zones, you can stop and start local zones. For more information, see “Starting and Stopping Local Zones” on page 213.




In order to perform actions on virtual servers, the virtual server's hypervisor must be reachable – that is, the Opware Agent installed on it must be reachable. Also, in order to perform actions on virtual servers, they also must have a reachable Opware Agent installed on them.

For more information about the possible statuses of a virtual server inside the SAS Client, see “Virtual Server Status” on page 206. For more information about the Opware Agent, see the *Opware® SAS User's Guide: Server Automation*.

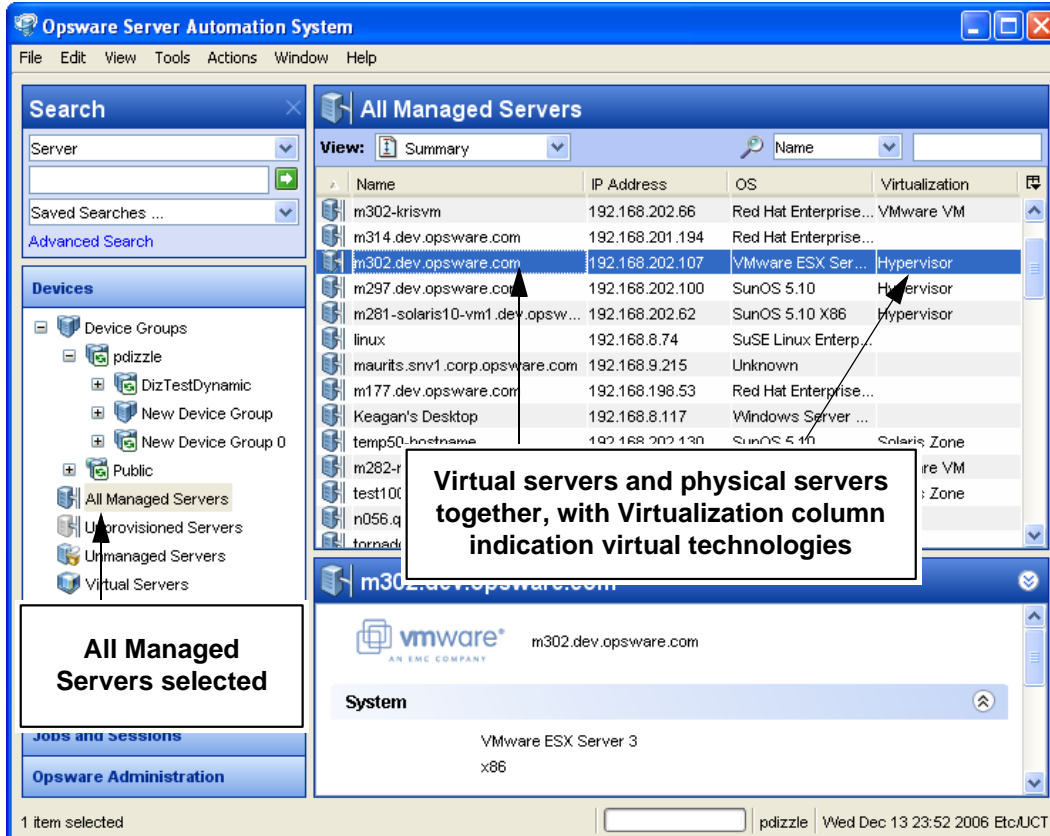
View Virtual Servers in All Managed Servers List

You can view virtual servers in the SAS Client in the all managed servers list, which combines all physical and virtual servers in one list. You will not see any hypervisor-virtual server relationships, but you can see if the server is virtual and whether it is a hypervisor or a virtual server.

To view virtual server information in the all managed servers list, select the column selector icon  at the right top of the Content pane and choose Virtualization. You will see the Virtualization column appear, and it will show the servers that are virtual servers and those that are hypervisors.

For example, Figure 6-2 illustrates the virtual servers and physical servers displayed from the all managed servers list.

Figure 6-2: All Managed Servers List Showing Physical and Virtual Servers Together



Refreshing Virtual Servers

From time to time, you should refresh your view of virtual servers so you can be sure that the data you are viewing is up to date and accurate.

For example, since the time you started viewing virtual servers in the Virtual Server list, someone else might have created a new virtual server, modified it, removed it, or stopped it. By refreshing your view of the list, you can be sure that you are working with an accurate picture of your virtual servers.

To refresh your view of virtual servers, perform the following steps:

- 1** From the Navigation pane, select the Devices tab.
- 2** Select the Virtual Servers list.

- 3** In the Content pane, select the Solaris 10 global zone hypervisor that you want to refresh, right-click, and select **Solaris Zones ► Refresh Zones**.
- 4** To refresh a VMware ESX hypervisor, select it from the Virtual Servers list, right-click, and select **VMWare Virtual Machines ► Refresh Virtual Machines**.

View Virtual Servers in the Device Explorer

To understand what the Device Explorer shows for the properties of a virtual server, see the following topics:

- Viewing Virtual Servers in Device Explorer–VMware ESX
- Viewing Virtual Servers in Device Explorer – Solaris 10

Viewing Virtual Servers in Device Explorer–VMware ESX

You can use the Device Explorer to view a VMware ESX VM or a hypervisor's server information. A VM as seen through the Device Explorer looks nearly the same as a regular physical server, except that it has an extra property named "Virtualization," which provides the following information:

- **Hypervisors:** When you view a VMware ESX hypervisor in the Device Explorer, you can see all of its hosted VMs.
- **VMware ESX VMs:** When you view a VMware ESX VM in the Device Explorer, the Virtualization view shows you the VM's virtual server properties, its virtual network configuration, and its data store configuration.

Figure 6-3 and Figure 6-4 illustrate the information that you can view for a VMware ESX hypervisor and VM in the Device Explorer.

Figure 6-3: VMware ESX Hypervisor Viewed in Device Explorer

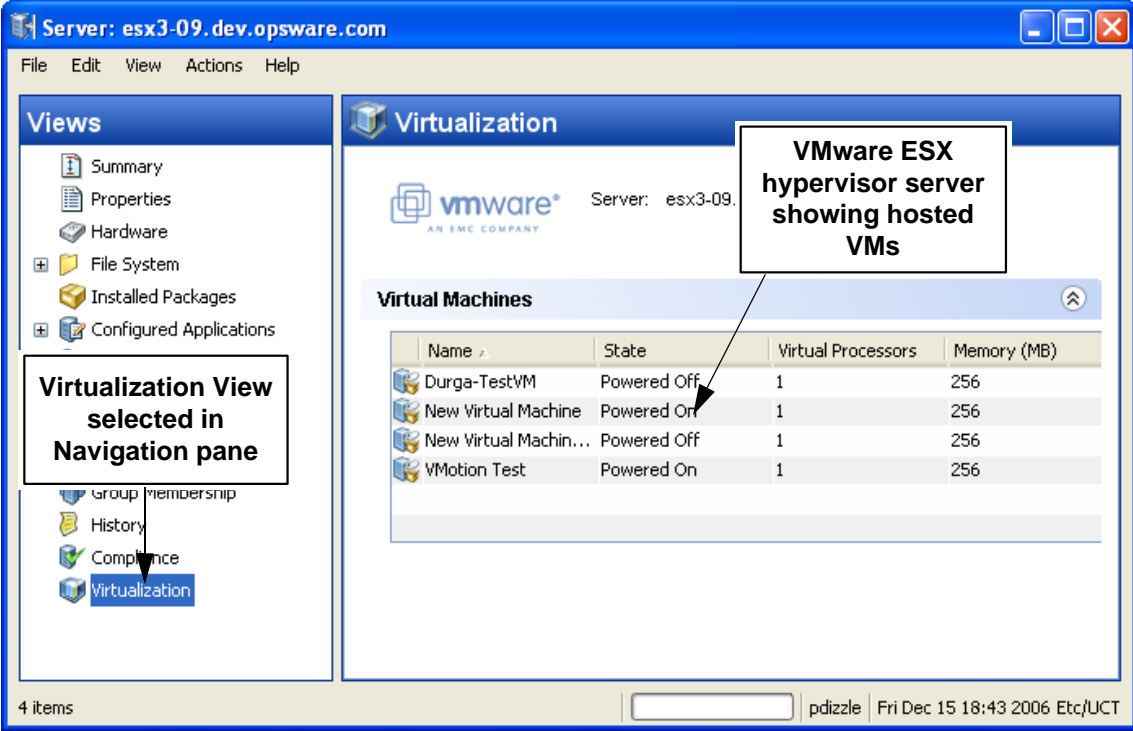
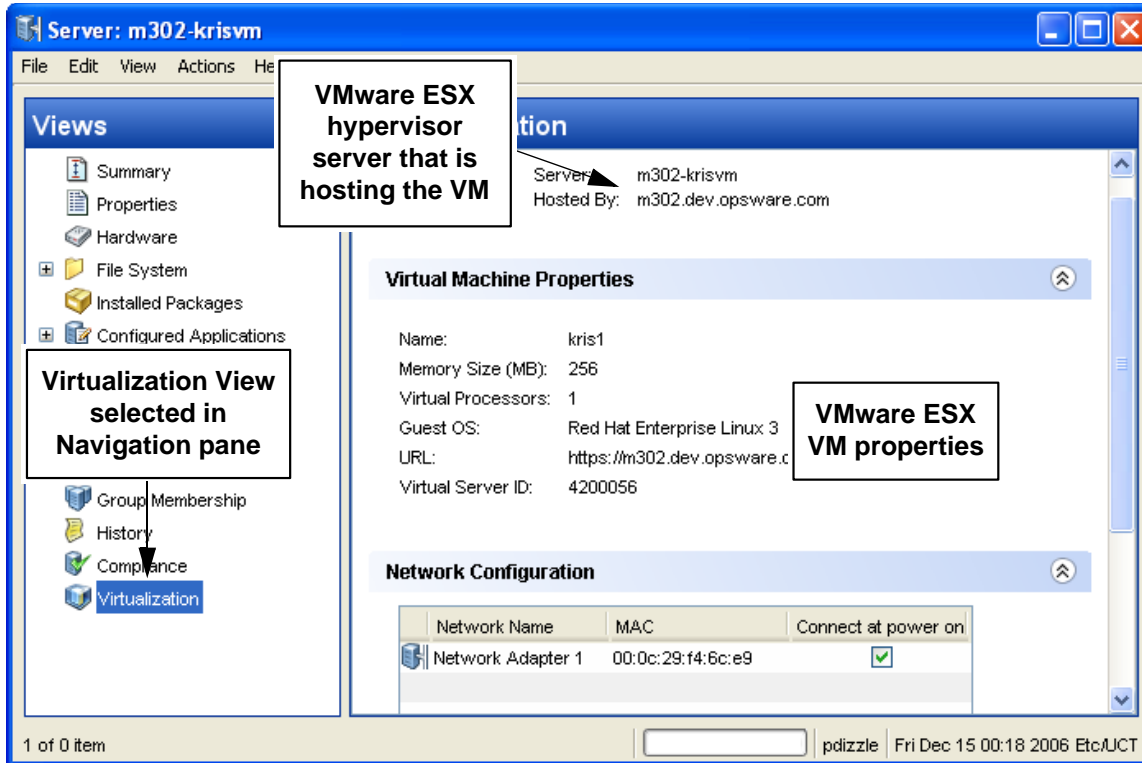


Figure 6-4: VMware ESX VM Viewed in Device Explorer



Viewing Virtual Servers in Device Explorer – Solaris 10

You can use the Device Explorer to view a Solaris 10 global zone hypervisor and local zone server information. A global zone or local zone as seen through the Device Explorer looks nearly the same as a regular physical server, except that it has an extra property named Virtualization which provides the following information:

- **Hypervisors:** When you view a Solaris 10 global zone hypervisor in the Device Explorer, the Virtualization view shows all hosted local zones. From here, you can also stop and start the local zones.
- **Solaris Local Zones:** When you view a Solaris local zone in the Device Explorer, the Virtualization view indicates the name of its hypervisor, its reserved CPU shares, and virtual hardware information.

Figure 6-5 and Figure 6-6 illustrate the information you can view for a Solaris 10 global zone hypervisor and a local zone in the Device Explorer.

Figure 6-5: Solaris 10 Hypervisor (Global Zone) Viewed in Device Explorer

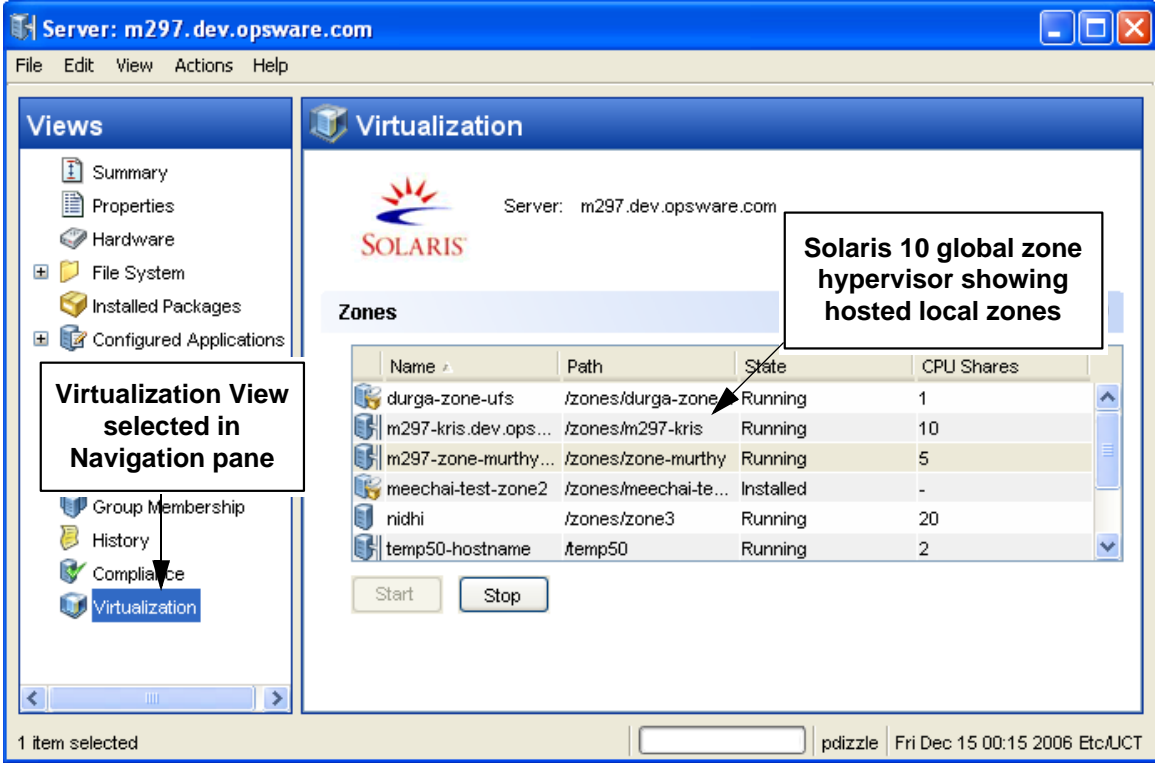
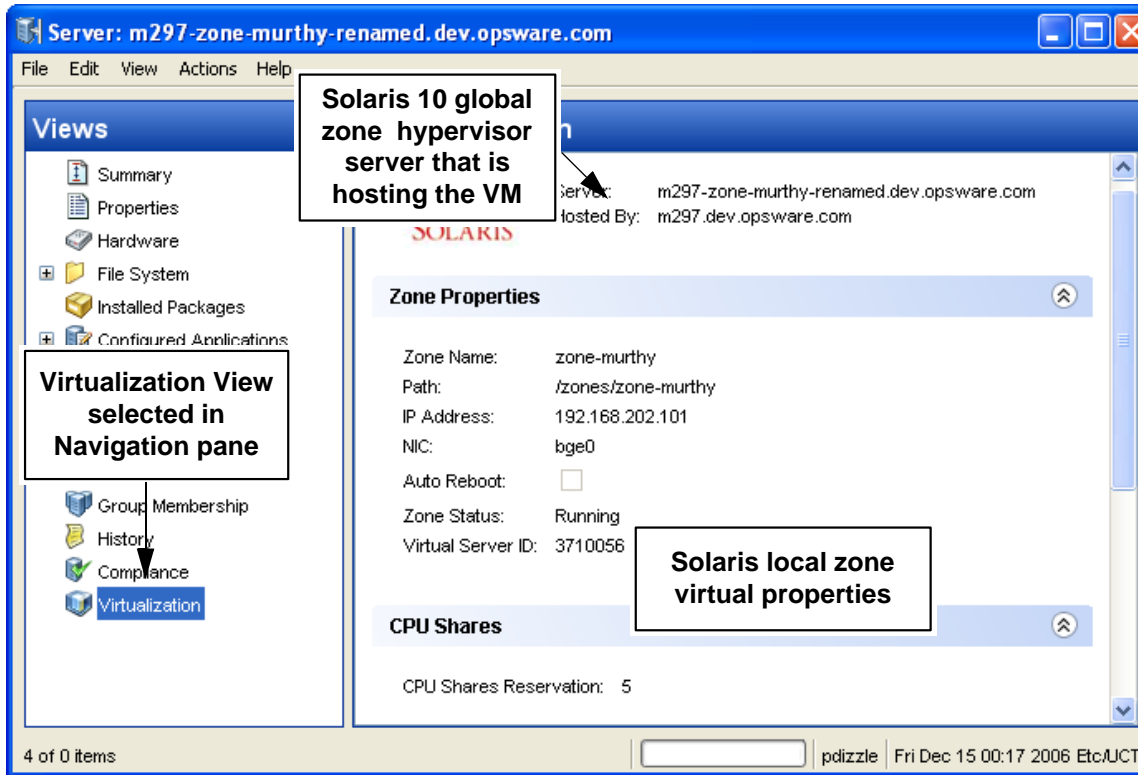


Figure 6-6: Solaris Local Zone Viewed in Device Explorer



View Virtual Server in Reports

From inside the SAS Client, you can generate the following reports to view virtual server information:

- **Virtual Servers by Virtualization Technology:** Shows all virtual servers by vendor, including Solaris 10 local zones and VMware ESX virtual machines (VMs).
- **All Virtual Servers:** Shows a list of all managed virtual servers in a table format, with a column named Hypervisor Name that lists the virtual server's hypervisor.
- **Virtual Servers by Hypervisor:** Shows all virtual servers grouped by hypervisor (Solaris Global Zones and VMware ESX hypervisors).
- **Resource Allocation by Hypervisor:** Shows resource allocation by hypervisor (Solaris Global Zones and VMware ESX hypervisors).

To generate reports to view virtual servers, perform the following steps:

- 1** From the Navigation pane, select Reports.
- 2** Expand the Reports folder and then expand a folder within it.
- 3** Select a report listed in the folder.
- 4** If there are no report parameters in the Content pane, click **Run**.
- 5** If there are report parameters in the Content pane, you can either use the default parameters or change them:
 - To use the default report parameters, click **Run** to run the report.
 - If you are running one of the resource allocation by hypervisor reports, from the hypervisor drop-down list, select a condition:
 - **Contains:** Enter text to search for matching characters that are contained in the hypervisor name, and then click **Run**.
 - **Equals:** Click the browse button to open a window that allows you to select a specific hypervisor by name, and then click **Run**.
 - **Begins With:** Enter text to search for matching characters that the hypervisor name begins with, and then click **Run**.
 - **Ends With:** Enter text to search for matching characters that the hypervisor name ends with, and then click **Run**.
- 6** (Optional) If the report results show a list of servers, then you can double-click the server name to open its device browser and view more details about the servers.
- 7** (Optional) If the report results show a pie chart, click on one of the sections of the chart, and drill down to a list of servers for that section. When you reach a list of servers, double-click a server name to open its device browser and view more details about the servers.

Virtual Servers in VAM

Using the Opware SAS Visual Application Manager (VAM) 2.0, you can view virtual servers and devices and their relationship to applications that run and depend upon them.

VAM is a tool that allows you to manage the operational architecture and behavior of distributed applications in your IT environment. VAM displays detailed application information in physical and logical drawings as a collection of component signatures, process families, connections, and dependencies and the relationship between all these elements.

Using VAM, you can view virtual servers and devices that your applications run on. VAM shows you how applications in your organization are connected to other virtual servers, hypervisors, and virtual switches.

Within VAM, you can view virtual servers in the Servers and Virtualization Maps – including VMware virtual machines, Solaris local zones, and the hypervisors that host them. For VMware ESX hypervisors, you can also view vSwitches alongside virtual machines, in addition to the connections between the virtual machines and vSwitches' port groups.

For more information on virtual servers in VAM, see Chapter 7, “Visual Application Manager” on page 59 of this guide.

Viewing Virtual Servers with VAM

To launch VAM from individual or multiple selected servers, virtual servers, or hypervisors, perform the following steps:

- 1** Launch the SAS Client from one of the following locations:
 - Click the SAS Client link in the Power Tools section of the SAS Web Client home page.
 - Double-click the SAS Client icon on your desktop (if you installed it on your desktop when you installed the SAS Client).
 - Select **Start** menu ► **All Programs** ► **Opware SAS Client**.
- 2** From the Navigation pane, select the Devices tab.
- 3** From the Device Groups, All Managed Servers list, or Virtual Servers list, select a server group, or one or more managed virtual servers or hypervisors by performing one of the following actions:

- From the **Actions** menu, select **Open with** ► **Visual Application Manager**.

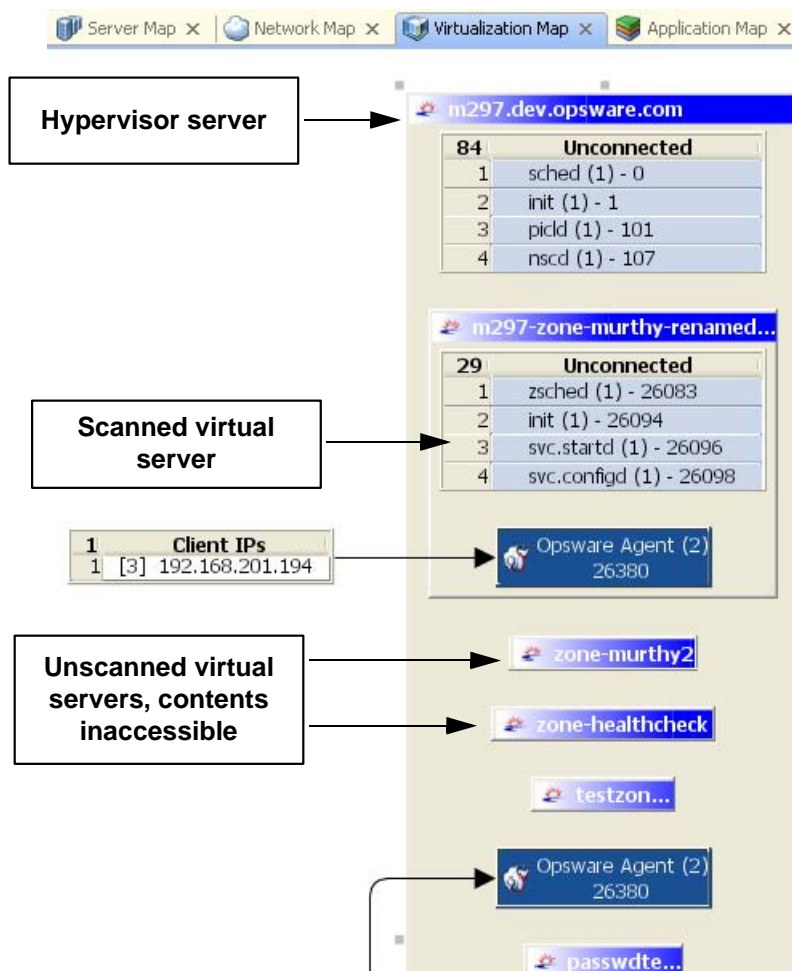
Or

- From the **Tools** menu, select **Visual Application Manager** ► **Open Selection**.

After scanning is completed, the VAM window appears displaying the selected servers.

Figure 6-7 illustrates how virtual servers appear in the Virtual Map, showing a Solaris global zone hypervisor with a collection of guest local zones contained within it.

Figure 6-7: Solaris Local Zones on a Global Zone Hypervisor as Visualized in VAM



Virtual Servers in the SAS Web Client

The SAS Web Client will show both hypervisors and virtual servers, but it will not show any virtual server relationships. You will be able to view virtual server and hypervisor properties, just like any other server under Opware management. You can view them as they move through the Opware Lifecycle states, such as planned, unprovisioned, managed, unreachable, and so on.

For more information on server management in the SAS Web Client, see *Opware® SAS User's Guide: Server Automation*.

Virtual Server Status

To perform actions on virtual servers, the virtual server's hypervisor must be reachable – that is, the Opware Agent installed on it must be reachable. Also, the virtual servers being hosted on the hypervisor must also have a reachable Opware Agent, just like a regular physical server.

For Solaris 10, when you create a new local zone using the SAS Client, a new Opware Agent is installed. (Currently, you cannot use the SAS Client to create a new VM on a VMware ESX hypervisor.) It is also possible that other users might have created new virtual servers (Solaris local zones or VMware ESX VMs) on a hypervisor outside of the SAS Client – and so these new virtual servers will need agents on them if you want to manage them.

And it is also possible that you will see a hypervisor that is not currently being managed by Opware – this means that for whatever reason, the Opware Agent on the hypervisor is not reachable, and thus you will not be able to perform any actions on the virtual servers being hosted on the hypervisor.

For information on how to install an Opware Agent on a Solaris local zone virtual server (you cannot install an agent in a VMware ESX VM in this release), see “Installing an Opware Agent on Unmanaged Solaris Local Zone” on page 212 and “Creating a Local Zone” on page 214. You can also use the Opware Agent Discovery and Deployment (ODAD) tool to install an Opware agent on an unmanaged virtual server. For more information, see Chapter 4, “Opware Agent Management”.

For information on how to troubleshoot an unreachable Opware Agent, see *Opware® SAS User's Guide: Server Automation*.

Virtual Server States

Table 6-6 describes the server states for virtual servers.

Table 6-6: Server Status Icons in Opware SAS




SERVER ICON	DESCRIPTION
	<p>Planned</p> <p>Indicates that a device record has been created for the server, but an Opware OS Build Agent has not yet been installed on it. Servers in this stage cannot be provisioned until the OS Build Agent is installed.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Unprovisioned – Unreachable</p> <p>Indicates a server that has been registered with the core via the Opware OS Build Agent, but has not reported as ready for provisioning recently. This may be due to networking problems between the server and the Opware core or the server having been disconnected or powered off.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Unprovisioned – Reachable</p> <p>Indicates a server that has been registered with the core via the Opware OS Build Agent and is available to have a target OS installed on it.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>

Table 6-6: Server Status Icons in Opsware SAS





SERVER ICON	DESCRIPTION
	<p>Provisioning – Unreachable</p> <p>Indicates a server on which the OS Provisioning feature was in the process of installing the target OS, but for some reason stopped because the server is unable to communicate with the Opsware core.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Provisioning – Reachable</p> <p>Indicates a server on which the OS Provisioning feature is in the process of installing the target OS.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Provisioning Failed – Unreachable</p> <p>Indicates an available server on which an error occurred while the OS Provisioning Subsystem was installing a target OS, and that the server is not able to communicate with the Opsware core.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Provisioning Failed – Reachable</p> <p>Indicates an available server on which an error occurred while the OS Provisioning Subsystem was installing a target OS.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>

Table 6-6: Server Status Icons in Opsware SAS



SERVER ICON	DESCRIPTION
	<p>Managed – Reachable</p> <p>Indicates a server has an An Opsware Agent is running on it and that it is able to communicate with the Opsware core.</p> <p>In the SAS Client, appears in the All Managed Servers list and Virtual Servers list.</p> <p>In the SAS Web Client, appears in the My Jobs panel in the home page, in the list in the My Jobs page, in the Manage Servers list, and in the server lists in the Opsware wizards.</p>
	<p>Managed – Unreachable</p> <p>Indicates a managed server cannot communicate with the Opsware core (it is Not Reachable).</p> <p>If you want to discover reasons why the managed server is unreachable, you can run a Communication Test. See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for more information.</p> <p>In the SAS Client, appears in the All Managed Servers list and Virtual Servers list.</p> <p>In the SAS Web Client, appears in the My Jobs panel in the home page, in the list in the My Jobs page, in the Manage Servers list, and in the server lists in the Opsware wizards.</p>

Table 6-6: Server Status Icons in Opware SAS












SERVER ICON	DESCRIPTION
	<p>Unmanaged</p> <p>Indicates the server is unmanaged, which means it does not have an Opware agent installed on it.</p> <p>For unmanaged virtual servers, this means that someone created a VMware Virtual Machine (VM) or Solaris local zone outside of Opware SAS and thus does not have an Opware Agent installed on it.</p> <p>For virtual servers, this state could also mean that the VMware VM is has not yet been provisioned, or that your user belongs to a group that does not have permissions to perform operations on this virtual server.</p> <p>For more information on installing an Opware agent on an unmanaged server, see Chapter 4, “Opware Agent Management” on page 99 of this guide</p>
	<p>Deactivated</p> <p>Indicates a server that was deactivated in Opware SAS so that it is currently not managed and is no longer reachable.</p> <p>Appears in the Manage Servers list and in the server lists in the Opware wizards (however, it is not selectable in the wizards).</p>
	<p>Scheduled</p> <p>Indicates a server that is scheduled for an operation (install software, uninstall software, and so forth).</p> <p>In the SAS Client, appears in the Job Logs list.</p> <p>In the SAS Web Client, appears in the My Jobs panel in the home page and in the list in the My Jobs page.</p>
	<p>Error</p> <p>Indicates a managed server on which an error occurred while Opware SAS was installing or uninstalling software.</p> <p>Appears in the My Jobs panel in the home page and in the list in the My Jobs page.</p>

Table 6-6: Server Status Icons in Opsware SAS

SERVER ICON	DESCRIPTION
	<p>Warning</p> <p>Indicates a managed server on which a warning occurred while Opsware SAS was installing or uninstalling software.</p> <p>Appears in the My Jobs panel in the home page and in the list in the My Jobs page.</p>
	<p>Application Configuration Out of Sync</p> <p>Indicates a managed server on which the configuration file on the server is out of sync with the Application Configuration Template (Opsware model).</p> <p>Appears only in the Application Configuration feature and the server list in the SAS Client.</p>
	<p>Static Device Group</p> <p>Indicates a static server group. The same states that apply to single servers apply to groups.</p> <p>See “Server Groups” on page 280 in this chapter for information about the different types of server groups.</p>
	<p>Dynamic Device Group</p> <p>Indicates a dynamic server group. The same states that apply to single servers apply to groups.</p>
	<p>Public Static Device Group</p> <p>Indicates a public and static server group. The same states that apply to single servers apply to groups.</p>
	<p>Public Edenic Device Group</p> <p>Indicates a public and dynamic server group. The same states that apply to single servers apply to groups.</p>

Installing an Opware Agent on Unmanaged Solaris Local Zone



For Solaris 10 local zones, if someone outside of the SAS Client has created a local zone, or if someone has uninstalled the Opware Agent from a previously managed local zone virtual server, it will appear as an unmanaged server.

This is indicated with the unmanaged server icon . Unless the local zone is managed (has a reachable Opware Agent installed on it), you will not be able to operate on the server.



You can only install an Opware Agent on an unmanaged local zone that is currently running. Also, all services on the local zone must be up and running. Keep in mind that it is possible that the local zone is running but not all services are up. If not all the services are up and running, one reason might be that the sysconfig information has not been provided to the local zone. The sysconfig information is provided by a user when the local zone is booted for the first time. See the Sun Solaris 10 documentation on zone configuration for more information

To install an Opware Agent on an unmanaged Solaris local zone, perform the following steps.

- 1** From inside the SAS Client, from the Navigation pane, select **Devices ► Virtual Servers**.
- 2** From inside the Content pane, expand the Solaris hypervisor server that contains the unmanaged local zone.
- 3** Select the unmanaged local zone (indicated with the unmanaged server icon ) , right-click, and select **Solaris Zones ► Install Agent**.
- 4** You will see the Install Agent window. If you want, click **Run in Background**. When the agent has finished installing successfully, the Status column will show a green check icon . If you see a failure status, contact your Opware administrator.
- 5** Click **Close**.

Solaris Local Zone Management

The SAS Client allows you to perform the following Solaris 10 local zone management tasks:

- Starting and Stopping Local Zones
- Creating a Local Zone
- Modifying a Local Zone
- Removing a Local Zone

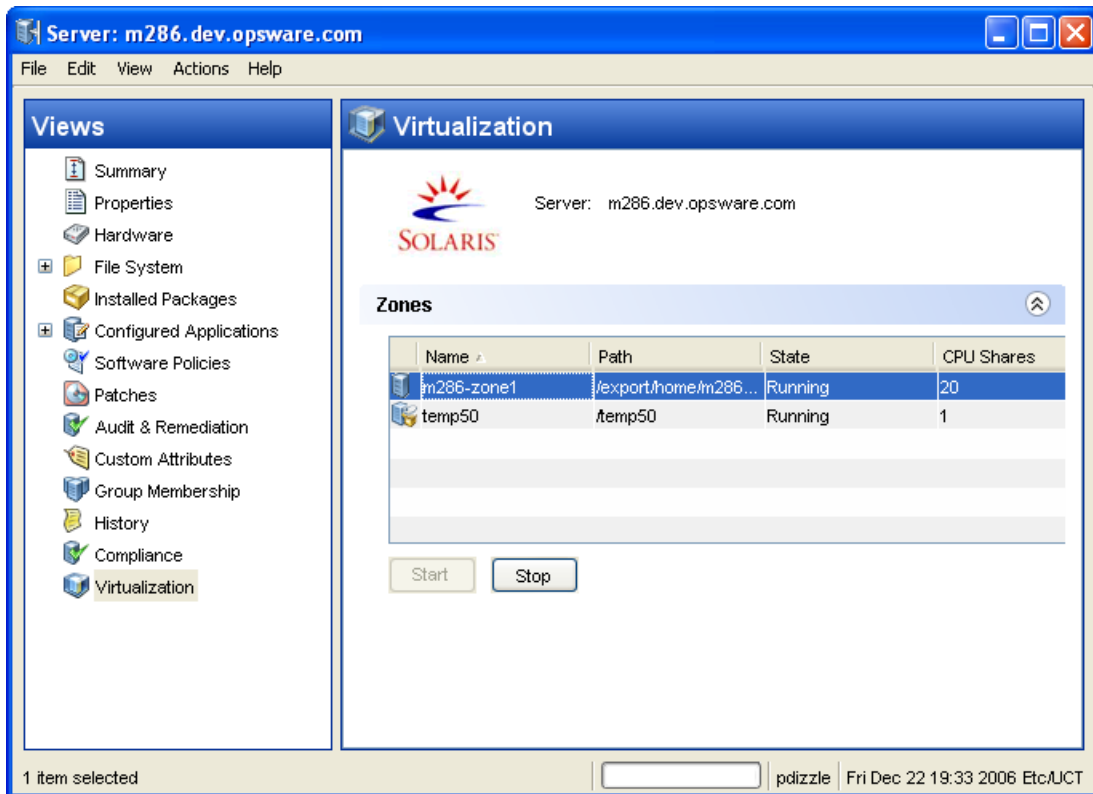
Starting and Stopping Local Zones

To start or stop a local zone, perform the following steps:

- 1** From the Navigation pane, select the Devices tab.
- 2** Select the Virtual Servers list.
- 3** In the Content pane, select a Solaris 10 global zone hypervisor.
- 4** Expand the hypervisor server, and select a local zone, right-click, and select **Solaris Zones ► Stop Zone**.
- 5** To start the zone, select it, right-click, and select **Solaris Zones ► Start Zone**.

- 6 (Optional) You can also stop and start a local zone from the Device Explorer of the Solaris 10 global zone hypervisor. To do so, from the Virtualization view, select a local zone in the list and click either **Start** or **Stop**, as shown in Figure 6-8.

Figure 6-8: Stopping or Starting a Local Zone from a Global Zone Hypervisor Device Browser



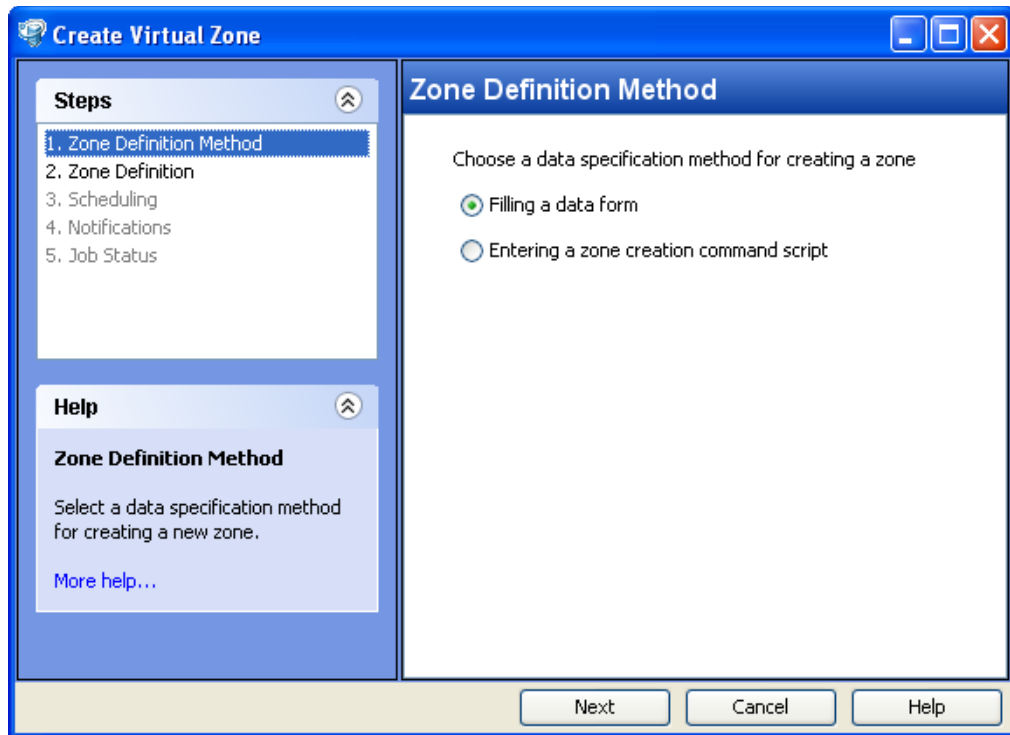
A Solaris local zone that is not running will show a state of "Installed" in the Device Explorer ► Virtualization view.

Creating a Local Zone

The SAS Client allows you create (and configure) a new, fully operable local zone on a Solaris 10 global zone hypervisor. When you create a new local zone on a Solaris 10 global zone, a new Opware Agent is installed and the local zone becomes manageable as a physical managed server in the SAS Client.

The Create Virtual Zone window allows you to configure and define all aspects of your local zone, such as its name, locale, time zone, terminal type, root password, CPU share, and so on. You can schedule the zone creation for a later date and configure email notifications to be sent after the zone has been created.

Figure 6-9: Create Virtual Zone Window



Using the Create Virtual Zone window, you can create a local zone by performing the following tasks:

- Launching the Create Virtual Zone Window
- Choosing Zone Definition Method
- Defining the Zone
- Scheduling Zone Creation
- Setting Email Notifications for Zone Creation
- Starting Zone Creation Job

Launching the Create Virtual Zone Window

The first step in creating a new local zone is launching the Create Virtual Zone window. To do so, perform the following steps:

- 1** Launch the SAS Client from one of the following locations:
 - Click the SAS Client link in the Power Tools section of the SAS Web Client home page.
 - Double-click the SAS Client icon on your desktop (if you installed it on your desktop when you installed the SAS Client).
 - Select **Start** menu ► **All Programs** ► **Opware SAS Client**.
- 2** From the Navigation pane, select the Devices tab.
- 3** Select the Virtual Servers list.
- 4** In the Content pane, select the Solaris 10 global zone hypervisor that you want to create a new local zone on, right-click, and select **Solaris Zones** ► **Create Zone**.
- 5** Once the Create Virtual Zone window is open, you need to choose a zone definition method.

Choosing Zone Definition Method

To choose a zone definition method, perform the following steps:

- 1** In the Create Virtual Zone window, step one, select one of the following zone creation methods:
 - **Filling Out a Data Form:** This option allows you to manually enter all of the zone creation configuration parameters.
 - **Entering a Zone Creation Command Script:** This option allows you to enter or upload a zone creation command script, which contains all the necessary zone creation configuration parameters. (This corresponds to running the `zoncfg -f` command if you were creating this local zone manually. The Create Virtual Zone feature does not validate a zone configuration command script, so make sure that the script you enter is a script that would work through the "`zoncfg -f [command file]`" argument. See the Sun Solaris 10 documentation on zone configuration for more information.)
- 2** Select a zone creation method and then click **Next** to proceed to the next window and define the zone.

Defining the Zone

In this step, you need to enter all the necessary configuration parameters that define the local zone.

To define the zone, perform the following steps:

- 1** In the Create Virtual Zone window, step two, fill out the following fields (all fields are required unless otherwise indicated as optional):
 - **Server:** Enter a server name for the new virtual server. (Beneath the server name, you can see the global zone that will be hosting this new local zone.)
 - **Zone Name:** Enter a name for the local zone. You might want to give the local zone a name that indicates what it is going to be used for, such as the application name that will be running in the zone.
 - **Terminal Type:** Specify the terminal client that the SAS Client uses for Remote Terminal sessions on the local zone.
 - **Auto Reboot:** Select to automatically reboot the local zone if the global zone physical server is rebooted.
 - **Locale:** Enter an encoding type for the local zone.
 - **Time Zone:** Select a time zone for the local zone.
 - **Root Password:** Enter the root password for logging into the local zone.
 - **Confirm Password:** Enter the root password again.
- 2** If you chose the Enter a Zone Creation Command Script option, in the Zone Configuration Commands section, enter (or paste) the contents of the zone creation command script. Or, click **Import File** to import the zone creation command script. (This corresponds to running the `zonecfg -f` command if you were creating this local zone manually. See the Sun Solaris 10 documentation on zone configuration for more information.) Then, click **Next** and move to the next task, “Scheduling Zone Creation” on page 218.
- 3** If you chose to manually fill out the zone creation data form, then complete the rest of the zone definition form (all fields are required unless indicated as optional):
 - **CPU Shares Reservation:** Enter the amount of allocated CPU usage to designate to the zone.



For the CPU shares reservation to take effect, the Fair Share Scheduler (FSS) must be enabled on the Solaris 10 hypervisor server on which you are creating the new local zone.

- **Virtual Hardware:** In this section, enter all virtual hardware information to configure for the local zone.
 - **Virtual Network Interfaces and IP:** Click **Add** to enter the IP address and the name of the virtual network interface. Each local zone that requires network connectivity must have one or more dedicated IP addresses. These addresses are associated with the physical network interface on the global zone.
 - **Device:** (Optional) Click **Add** to enter a pathname to a device on the global zone hypervisor. This allows you to give the local zone access to a device on the global zone.
 - **Inherited Package Directory:** (Optional) Click **Add Sparse Root** to enter a default package directory to be inherited from the global zone to the local zone. Or, click **Add** to enter a pathname to the package directory you want the local zone to inherit.
 - **Mount File System:** (Optional) Click **Add** to mount a file system type and path for the local zone. The “ufs” file systems are used to create a file system mount within the local zone; the “lofs” will create a loopback file system mount to the global zone.
- 4** When you have finished filling out the zone creation form, click **Next** to proceed to the next window and schedule a zone creation job.

Scheduling Zone Creation

In this step, you can schedule the zone creation to run immediately or at a specified date and time.

To schedule the zone creation, perform the following steps:

- 1** From the Create Virtual Zone window, the Scheduling step displays the scheduling options for the zone installation.

Select one of the following Zone Creation options:



- **Run Task Immediately:** This option allows you to download or install immediately.
- **Run Task At:** This option allows you to specify the date and time to create the new local zone.

- 2 Click **Next** to proceed to the Notification step.

Setting Email Notifications for Zone Creation

In this step, you can set email notifications to alert users on the success or failure of a zone creation job. You can also associate a Ticket ID with the job.

To set email notifications, perform the following steps:

- 1 To add email addresses, click **Add Notifier** from the Notifications window, and enter the email addresses in the Notification Email Address field.
- 2 To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the zone creation phase.
- 3 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 4 Click **Next** to go to the Start Job step.

Starting Zone Creation Job

In this step, you can start the job, view the summary information of the job progress and see the individual status of each action required for the job to be completed.

To start the zone creation job, perform the following steps:

- 1 From the Create Virtual Zone window, click **Start Job** to create a new zone.
- 2 If you selected Run Task Immediately in the Scheduling step, the job begins immediately. If you scheduled the job for a later time, the job will run at the scheduled time. The job's progress appears in the Create Virtual Zone window.
- 3 To view the details of each action, select a row in the table. The details for each action appear.
- 4 Click **End Job** to stop the job from running or click **Close** to close the Create Virtual Zone window.
- 5 When the new local zone has been created, select Virtual Servers from the Navigation pane, and expand the contents of the hypervisor you created the local zone on, and you can see your new local zone.



You can also view all your jobs from the job logs in the SAS Client. See the *Opware® SAS User's Guide: Server Automation* for information about job logs.

Modifying a Local Zone

You can use the Modify Zone window to modify a subset of the zone definition parameters that were defined when a zone was created. Once you make modifications to the zone, you can run the zone modification immediately or schedule it for a later time, and you can also configure notification emails to be sent when the job is finished.

Modifying a local zone consists of the following tasks:

- Launching the Zone Modification Window
- Modifying the Zone Definition
- Scheduling a Zone Modification Job
- Setting Email Notifications for Zone Modification
- Starting a Zone Modification Job

Launching the Zone Modification Window

The first step in modifying a local zone is launching the Modify Virtual Zone window. To do so, perform the following steps:

- 1** Launch the SAS Client from one of the following locations:
 - Click the SAS Client link in the Power Tools section of the SAS Web Client home page.
 - Double-click the SAS Client icon on your desktop (if you installed it on your desktop when you installed the SAS Client).
 - Select **Start** menu ► **All Programs** ► **Opware SAS Client**.
- 2** From the Navigation pane, select the Devices tab.
- 3** Select the Virtual Servers list.
- 4** In the Content pane, select the Solaris 10 global zone hypervisor that you want to create a new local zone on, right-click, and select **Solaris Zones** ► **Modify Zone**.
- 5** Once the Create Virtual Zone window is open, you can edit the zone definition.

Modifying the Zone Definition

To modify the zone definition, perform the following steps:

- 1 In the Modify Virtual Zone window, step one, modify the following parameters:
 - **Auto Reboot:** Select to automatically reboot the local zone if the global zone physical server is rebooted.
 - **CPU Shares Reservation:** Enter the amount of allocated CPU usage to designate to the zone.



For the CPU shares reservation to take effect, the Fair Share Scheduler (FSS) must be enabled on the Solaris 10 hypervisor server on which you are creating the new local zone.

- **Virtual Hardware:** In this section, enter all virtual hardware information to configure for the local zone.
 - **Virtual Network Interfaces and IP:** Click **Add** to enter the IP address and the name of the virtual network interface. Each local zone that requires network connectivity must have one or more dedicated IP addresses. These addresses are associated with the physical network interface on the global zone.
 - **Device:** (Optional) Click **Add** to enter a pathname to a device on the global zone hypervisor. This allows you to give the local zone access to a device on the global zone.
 - **Inherited Package Directory:** (Optional) Click **Add Sparse Root** to enter a default package directory to be inherited from the global zone to the local zone. Or, click **Add** to enter a pathname to the package directory you want the local zone to inherit.
 - **Mount File System:** (Optional) Click **Add** to mount a file system type and path for the local zone. The “ufs” file systems are used to create a file system mount within the local zone; the “lofs” will create a loopback file system mount to the global zone.
- 2 When you have finished filling out the zone creation form, click **Next** to proceed to the next window and schedule the zone modification job.

Scheduling a Zone Modification Job

In this step, you can schedule the zone modification to be run immediately or at a specified date and time.

To schedule the zone modification, perform the following steps:

- 1** From the Modify Virtual Zone window, the Scheduling step displays the scheduling options for the zone modification.

Select one of the following Zone Modifications options:



- **Run Task Immediately:** This option allows you to run the zone modification job.
- **Run Task At:** This option allows you to specify the date and time to start the zone modification job.

- 2** Click **Next** to proceed to the Notification step.

Setting Email Notifications for Zone Modification

In this step, you can set email notifications to alert users on the success or failure of the zone modification job. You can also associate a Ticket ID with the job.

To set email notifications, perform the following steps:

- 1** to add email addresses, click **Add Notifier** from the Notifications window, and enter the email addresses in the Notification Email Address field.
- 2** To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the zone modification phase.
- 3** Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 4** Click **Next** to go to the Start Job step.

Starting a Zone Modification Job

In this step, you can start the zone modification job, view the summary information of the job progress, or view the individual status of each action required for the job to complete.

To start the zone modification job, perform the following steps:

- 1** From the Modify Virtual Zone window, click **Start Job** to modify the local zone.

- 2 If you selected Run Task Immediately in the Scheduling step, the job begins immediately. If you scheduled the job for a later time, the job will run at the scheduled time. The job's progress appears in the Modify Virtual Zone window.
- 3 To view the details of each action, select a row in the table. The details for each action appear.
- 4 Click **End Job** to stop the job from running or click **Close** to close the Modify Virtual Zone window.

Removing a Local Zone

You can use the Remove Virtual Zone window to remove a local zone from a Solaris 10 global zone hypervisor. To remove a zone, perform the following tasks:

- Launching the Zone Removal Window
- Scheduling Zone Removal Job
- Setting Email Notifications for Zone Removal
- Starting Zone Removal Job

Launching the Zone Removal Window

The first step in removing a local zone is launching the Remove Virtual Zone window. To do so, perform the following steps:

- 1 Launch the SAS Client from one of the following locations:
 - Click the SAS Client link in the Power Tools section of the SAS Web Client home page.
 - Double-click the SAS Client icon on your desktop (if you installed it on your desktop when you installed the SAS Client).
 - Select **Start** menu ► **All Programs** ► **Opware SAS Client**.
- 2 From the Navigation pane, select the Devices tab.
- 3 Select the Virtual Servers list.
- 4 In the Content pane, select the Solaris 10 global zone hypervisor that you want to create a new local zone on, right-click, and select **Solaris Zones** ► **Remove Zone**.

Once the Remove Virtual Zone window is open, you can schedule the zone removal job.

Scheduling Zone Removal Job

In this step, you can schedule the zone removal to be run immediately or at a specified date and time.

To schedule the zone removal, perform the following steps:

- 1** From the Remove Virtual Zone window, the Scheduling step displays the scheduling options for the zone removal.

Select one of the following Zone Removal options:

- **Run Task Immediately:** This option allows you to run the zone removal job.
- **Run Task At:** This option allows you to specify the date and time to start the zone removal job.



- 2** Click **Next** to proceed to the Notification step.

Setting Email Notifications for Zone Removal

In this step, you can set email notifications to alert users on the success or failure of a zone removal job. You can also associate a Ticket ID with the job.

To set email removal, perform the following steps:

- 1** To add email addresses, click **Add Notifier** from the Notifications window, and enter the email addresses in the Notification Email Address field.

- 2** To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the zone removal phase.

- 3** Enter a Ticket ID to be associated with a Job in the Ticket ID field.

- 4** Click **Next** to go to the Start Job step.

Starting Zone Removal Job

In this step, you can start the zone removal job, view the summary information for the job progress and see the individual status of each action required for the job to complete.

To start the zone removal job, perform the following steps:

- 1** From the Remove Virtual Zone window, click **Start Job** to remove a local zone.

If you selected Run Task Immediately in the Scheduling step, the job begins immediately. If you scheduled the job for a later time, the job will run at the scheduled time. The job progress appears in the Remove Virtual Zone window.
- 2** To view the details of each action, select a row in the table. The details for each action appear.
- 3** Click **End Job** to stop the job from running or click **Close** to close the Remove Virtual Zone window.

Searching for Virtual Servers

Because Opware SAS allows you to manage hundreds, even thousands of servers, the SAS Client search tool gives you the ability to search for servers and find the ones you are looking for.

To find specific virtual servers in your data center, you can search for them using some of the following criteria:

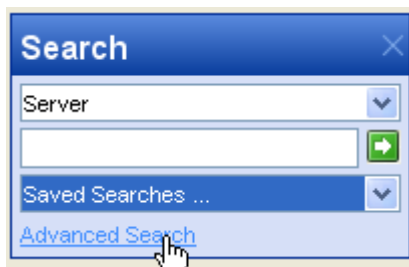
- **Generic virtualization criteria:** You can search for the type of server, such as a hypervisor, a Solaris local zone or a VMware ESX VM.
- **VMware specific criteria:** You can search for a VM's name, data store name, memory, virtual processors, and so on.
- **Solaris 10 local zone criteria:** You can search for a local zone's name, path, CPU shares, auto reboot setting, and so on.
- **Combinations or virtualization criteria:** You can search for all local zones that have CPU Shares of greater than 10 (or any other Zone attribute) AND are running Solaris 10 (or any other managed server attribute). Or, you can search for hypervisors that have more than eight local zones running on them, and so on.

One useful way to save the results of your search is to create a Device Group based on the search results. For more information on creating a Device Group, see "Creating Device Groups for Virtual Servers" on page 228.

To search for virtual servers in your data center using the SAS Client, perform the following steps:

- 1** From the Navigation pane, select Search.
- 2** If the Search tool is not visible, then select **Search Pane** from the **View** menu.
- 3** Click the Advanced Search link at the bottom of the search tool, as shown in Figure 6-10.

Figure 6-10: Simple Search Tool in the SAS Client



- 4** The Advanced Search pane appears to the right, which allows you to enter more specific criteria for virtual servers. From the first drop-down list to the left, select Server.
- 5** From the next drop-down list to the right, select a virtual server parameter, such as VM name, data store name, memory, virtual processors. Or, for Solaris local zones, you can select the name, path, CPU shares, auto reboot setting, and so on. For some parameters, you will need to select the criteria from the Select Values window, which requires selecting a value from the left pane and clicking the arrow button to include the parameters in the search.

- 6** Click **Search**. The search results appear in the Content pane. For example, Figure 6-11 shows the results of a search for all Solaris local zones in the data center.

Figure 6-11: Search Results for All Solaris Local Zones

The screenshot shows the 'Advanced Search' window. At the top, there are dropdown menus for 'Server', 'Virtualization Type', and 'Equals', with a text input field containing 'Solaris Zone'. Below these are buttons for 'Save...', 'Export...', 'Search', 'Reset', and 'Cancel'. The main area displays a table of search results with columns: Name, Serial Number, IP Address (Pri...), Operating Syst..., Manufacturer, Model, and Hostname. The results list five entries, all identified as 'SOLARIS ZONE' by the manufacturer and model.

Name	Serial Number	IP Address (Pri...)	Operating Syst...	Manufacturer	Model	Hostname
m286-zone1	80D9A8D6-M2...	192.168.202.74	SunOS 5.10	SUN MICROSY...	SOLARIS ZONE	m286-zone1
m293-apache-...	835A5AC1-AP...	192.168.202.98	SunOS 5.10	SUN MICROSY...	SOLARIS ZONE	m293-apache-...
m293-oracle-z...	835A5AC1-OR...	192.168.202.96	SunOS 5.10	SUN MICROSY...	SOLARIS ZONE	m293-oracle-z...
m293-weblogic...	835A5AC1-M2...	192.168.202.97	SunOS 5.10	SUN MICROSY...	SOLARIS ZONE	m293-weblogic...
temp51	80D9A8D6-TE...	192.168.202.73	SunOS 5.10	SUN MICROSY...	SOLARIS ZONE	temp51

- 7** (Optional) You can now perform the actions on your search results:
- Click on any column heading to sort the search results. You can also change the order of the columns by dragging the column heading and dropping it into the desired location.
 - Click **Save** to save your search query. The Save Search window appears. Enter the name of the search and click **Save**. The name of the saved search cannot be more than 64 characters.
 - When you save the search results, you can also choose to save the results as a static or dynamic device group. Click **Save**. In the Save Search window, from the Search Type drop-down list, select Dynamic Device Group or Static Device Group. If you choose the Dynamic Device Group, then the search parameters will be used as rules that determine the membership of the dynamic group. For example, if you saved a search for all Solaris local zones as a dynamic device group, then the group will include in its membership all local zones in your data center.
 - Click **Export** to export search results. The Export Results window appears. Enter the location, the file name and the file type and then click **Export Results**.



- After you export the search results, you can email the search results by attaching the exported file to the email. You can also print the search results by printing the exported file from an application that supports .csv or .html files.
- To perform an action on the search results, select an item from the Content pane and then from the **Actions** menu, select the appropriate action.

Creating Device Groups for Virtual Servers

A useful method to keep track of and operate on your virtual servers is to create device groups for them.

Device groups can be used as a shortcut for performing the same action on all of the servers simultaneously, instead of performing the action on each individual server. Server groups can also be used to simply organize groups of servers.

Device Groups can be either static or dynamic:

- **Static Device Groups** : These contain servers that are added to and removed from the group manually (as opposed to being added based upon user-defined rules). When using static groups, you first create the group, and then select the servers to populate it.
- **Dynamic Device Groups** : These contain servers added to or removed from the group based on a set of user-defined rules. If the rules are changed or the servers in the environment change, servers will be added to or removed from the group automatically. Rules apply only to the group being created or modified, not to any subgroups.

To create a device group for virtual servers, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups**.
- 2** From Device Groups, select either **Public** or your own private groups.
- 3** From the **Actions** menu, select **New** ► **Static Device Group** or **Dynamic Device Group**.
- 4** The new group appears in the Content pane. Enter a name for the group and then press **Enter** on your keyboard.
- 5** From the Navigation pane, select the new group and from the **Actions** menu, select **Open**.

6 In the Device Groups Browser, the type of group you created – static or dynamic – determines how you configure the group membership. If you created a static device group, from the Device Browser's View pane (left side), select Server Membership. In the Content pane of the Device Browser, right-click and select **Add Members**. Select the virtual servers to add to the group and then click **Add to Group**.

7 If you created a dynamic device group, from the Device Browser's View pane (left side), select Server Membership. In the Content pane of the Device Groups Browser, select the parameters for the group you want to use to determine the group membership.

For example, from the first drop-down list on the left, select a virtual server parameter, such as VM name, data store name, memory, or virtual processors. (For Solaris local zones, you can select the name, path, CPU shares, auto reboot setting, and so on.) For some parameters, you will need to select the criteria from the Select Values window, which requires selecting a value from the left pane and clicking the arrow button to include the parameters in the search.

8 You can continue to add filtering parameters by clicking the plus (+) button, or click the minus (-) button to remove them. When you are finished configuring the dynamic device group rules, click **Preview**. If any servers are found, they will become members of the group. Any new servers that are added to your data center under Opsware management that meet this criteria will be added to the group. Any servers that fail to meet the criteria will be automatically removed.

9 From the **File** menu, select **Save**.

Chapter 7: Server Tracking in the SAS Web Client

IN THIS CHAPTER

This section discusses the following topics:

- Server Tracking
- Server Lists
- My Servers
- Server Search
- Server Identification
- Server Histories and Reports
- Hardware Information for Managed Servers

Server Tracking

This section discusses the following topics:

- Ways to Locate, List, and Display Servers
- Tracked Server Properties
- Supported Operating Systems for Managed Servers.

Ways to Locate, List, and Display Servers

You can locate, list, and display servers in the SAS Web Client in the following four ways:

- By searching when you know the name, host name, or IP address of the server you want to provision or manage.
- By viewing the Manage Servers list and Server Pool list when you want to see a complete list of all your servers. You can refine the lists by using filters.

- By viewing servers sorted by hardware category. (Click Environment ► Hardware in the navigation panel.) The Servers tab in the Hardware pages shows each manufacturer and model that you have running in the operational environment. See “Hardware Information for Managed Servers” on page 270 in this chapter for more information.
- You can also browse managed servers and server groups using the SAS Client.

Tracked Server Properties

Every server that Opware SAS manages has the following properties:

- IP addresses, host name, and the server ID
- All software that is installed on the server. Select the Installed Packages tab from the Manage Servers: Server Properties page to display the list of software that is reportedly installed on the server.

Opware SAS is able to determine what software is installed on a server because the Opware Agent communicates with the Opware core and reports the installed hardware and software for the server.

In some cases, Solaris packages might only be partially installed. In these cases, the partially installed Solaris package does not show up in the installed list.

See “Server Information that the Opware Agent Tracks” on page 103 in Chapter 4 for information about a complete list of all the hardware and software information that Opware SAS tracks for managed servers.

Supported Operating Systems for Managed Servers

This section lists the supported operating systems for Opware Agents, the SAS Web Client, and the SAS Client.

The following table lists the supported operating systems for Opware Agents, which run on the servers managed by Opware SAS.

Table 7-1: Opware Agent Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR OPWARE AGENT	VERSIONS	ARCHITECTURE
AIX	AIX 4.3 AIX 5.1 AIX 5.2 AIX 5.3	POWER POWER POWER POWER
HP-UX	HP-UX 10.20 HP-UX 11.00 HP-UX 11.11 HP-UX 11.23 (11i v2)	PA-RISC PA-RISC PA-RISC PA-RISC and Itanium
Sun Solaris	Solaris 6 Solaris 7 Solaris 8 Solaris 9 Solaris 10 Solaris 10 Update 2 Solaris 10 Update 3	Sun SPARC Sun SPARC Sun SPARC Sun SPARC Sun SPARC, 64 bit x86 and Niagara Sun SPARC, 64 bit x86 and Niagara Sun SPARC, 64 bit x86 and Niagara
Fujitsu Solaris	Solaris 8 Solaris 9 Solaris 10	Fujitsu SPARC Fujitsu SPARC Fujitsu SPARC
Windows	Windows NT 4.0 Windows 2000 Server Family Windows Server 2003 Windows Server 2003 x64 Windows XP Professional	32 bit x86 32 bit x86 32 bit x86 64 bit x86 32 bit x86

Table 7-1: Opware Agent Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
Red Hat Linux	Red Hat Linux 7.3	32 bit x86
	Red Hat Linux 8.0	32 bit x86
	Red Hat Enterprise Linux 2.1 AS	32 bit x86
	Red Hat Enterprise Linux 2.1 ES	32 bit x86
	Red Hat Enterprise Linux 2.1 WS	32 bit x86
	Red Hat Enterprise Linux 3 AS	32 bit x86 and 64 bit x86 and Itanium
	Red Hat Enterprise Linux 3 ES	32 bit x86 and 64 bit x86 and Itanium
	Red Hat Enterprise Linux 3 WS	32 bit x86 and 64 bit x86 and Itanium
	Red Hat Enterprise Linux 4 AS	32 bit x86 and 64 bit x86
	Red Hat Enterprise Linux 4 ES	32 bit x86 and 64 bit x86
Red Hat Enterprise Linux 4WS	32 bit x86 and 64 bit x86	
SUSE Linux	SUSE Linux Enterprise Server 8	32 bit x86
	SUSE Linux Standard Server 8	32 bit x86
	SUSE Linux Enterprise Server 9	32 bit x86 and 64 bit x86
	SUSE Linux Enterprise Server 10	32 bit x86 and 64 bit x86
VMware	ESX Server 3	32 bit x86 and 64 bit x86

The following table lists the operating systems supported for the SAS Client.

Table 7-2: SAS Client Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR SAS CLIENT	VERSIONS	ARCHITECTURE
Windows	Windows XP	32 bit x86
	Windows 2003	32 bit x86
	Windows 2000	32 bit x86



Java J2SE v 1.4.2_13 JRE must be installed on the system that runs on the SAS Client. To download this version of Java, go to <http://java.sun.com/j2se/1.4.2/download.html>

Server Lists

This section discusses the following topics:

- Types of Server Lists
- Server Pool
- Manage Servers List
- Filters on the Manage Servers List

Types of Server Lists

The SAS Web Client displays lists for two types of servers, as Figure 7-1 shows.

Figure 7-1: Servers Section in the Navigation Panel



Server Pool: Servers in the Server Pool have registered their presence with Opware SAS but do not have the target OS installed. An OS Build Agent is running on each server so that they can communicate with Opware SAS.

See *Opware® SAS User's Guide: Application Automation* on how to use the Server Pool when you install the target OS on a server.

Manage Servers: The Manage Servers list contains servers on which Opware SAS can perform management tasks, because Opware Agents are installed on them. However, Opware SAS might not have provisioned all software running on the servers.

You begin the OS provisioning process by reviewing the servers in the Server Pool list. From the Server Pool, you can install a target OS by selecting a server and clicking **Install OS**.

Server Pool

The Server Pool provides the following information about each server waiting to be provisioned with the target OS:

- The host name set by booting the server for the first time over the network or by using an Opware Boot Floppy
- The MAC address
- The manufacturer and model
- The OS that the OS Build Agent is running – DOS (Windows operating systems), Linux, or Solaris

You use this information to select the target OS for servers. If the server is in the process of installing an OS, this value might change.

- The last date and time that the Opware Agent on the server communicated with Opware SAS (by submitting the server's hardware and software information)


If the server is in an unreachable state (that is, if the server icon has a red "x" on it), you can run a Communication Test to help you troubleshoot why that server is unreachable. See "Agent Reachability Communication Tests" on page 125 in Chapter 4 for more information.


- The life cycle value, such as whether the server is available to have a target OS installed on it
- The facility in which the server is located
- The customer association
- Additional hardware information (Click the server name to open a window that displays specific hardware information.)

Manage Servers List



The Manage Servers list contains servers on which Opsware SAS can perform management tasks because Opsware Agents are installed on them. When an existing operational server has an Opsware Agent installed successfully, it appears in the Manage Servers list and the server icon indicates that it is fully manageable, as Figure 7-2 shows.

Figure 7-2: The Manage Servers List in the SAS Web Client

Manage Servers (Summary View) 

All Statuses Red Hat Enterprise Linux AS 2.1 All Stages All Uses
 All Facilities All Customers All Manufacturers 
 All Models All Lifecycles

Resource Edit View Tasks Configuration Tracking

<input type="checkbox"/>	Name <input type="button" value="▲"/>	Host Name / IP Address	OS Version	Stage	Use	Facility	Customer
 Public Groups							
<input type="checkbox"/>	 m022.dev.opsware.com	m022.dev.opsware.com 192.168.197.91	Red Hat Enterprise Linux AS 2.1	Not Specified	Not Specified	C03	Not Assigned

See “Opsware Agent on Managed Servers” on page 99 in Chapter 4 for more information. By default, servers in the Manage Servers list are sorted by the Name column. However, you can re-sort the list based on any of the column headings. For example, you can click the Hostname / IP Address column heading to re-sort the list by host name or IP address.

If you have many servers that Opsware SAS manages, the list of servers is grouped by pages. Click the page number links or the left arrow at the bottom of the list.

The Manage Servers list provides the following information about each server:

- The name of the server
 - By default, the server's host name appears in this field. However, you can edit it so that it is more descriptive or useful.
- The host name of the server determined by the Opsware Agent
- The IP address configured for the server, which users can edit by using the network configuration feature in the
- The reported OS, which is obtained by the Opsware Agent that is running on the server
- The stage of the server, which specifies the stages of deployment for servers
- The server's use
- The facility in which the server is located

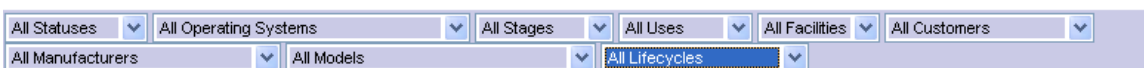
- The customer association
- Additional hardware information (Click the server name to open a window that displays specific hardware information.)

Filters on the Manage Servers List

The Manage Servers list displays the following filters that you can specify to qualify the servers that the SAS Web Client displays, as Figure 7-3 shows.

Figure 7-3: Filters in the Manage Servers List

Manage Servers (Summary View)



- **Status:** Specifies the ability of Opware SAS to manage servers. Opware SAS automatically detects the status of servers; a server's status is OK or Not Reachable.
- **OS:** Specifies the operating system on the server, which is obtained by the Opware Agent that is running on the server.
- **Stages:** Specifies the stages of deployment for servers; for example, a server is live or offline. Users set this property for servers. The values in this list are customizable by the Opware administrator.
- **Uses:** Specifies how an organization is utilizing servers; for example, a server is a staging server. Users set this property for servers. The Opware administrator can customize the values in this list.
- **Facilities:** Specifies the location of servers. From an SAS Web Client, users can manage servers located in any facility. For example, a user could log in to the SAS Web Client running in facility A and manage the server located in facility B.
- **Customers:** Specifies the customer associated with each server. Your Opware administrator defines the options for customer selections by using the Administration pages.
- **Manufacturers:** Specifies the manufacturer for the server as reported by the OS Build Agent running on the server.
- **Models:** Specifies the model of the server as reported by the OS Build Agent running on the server.

- **Life cycles:** Specifies the various Opsware server life cycle values which include Managed, Available, Build Failed, Installing OS, and Deactivated.



You can change the filters displayed in the Manage Servers page. To change the filters you want to be displayed on the Manage Servers page, click on the icon as shown in Figure 7-4 and specify the filters from the **Edit Filters** Menu.

Figure 7-4: Edit Icon



Figure 7-5 shows the filters that are in the Server Pool list.

Figure 7-5: Filters in the Server Pool List



- **Manufacturers:** Specifies the manufacturer for the server as reported by the OS Build Agent running on the server.
- **Models:** Specifies the model of the server as reported by the OS Build Agent running on the server.
- **Facilities:** Specifies the location of the server. Users can manage servers in any facility from an SAS Web Client in any facility.

My Servers

This section contains the following topics:

- Overview of My Servers
- Adding Servers to My Servers
- Removing Servers from My Servers

Overview of My Servers

The My Servers feature provides an efficient way to manage servers when your operational environment contains hundreds or thousands of servers.

When you search for servers or browse the server lists, you can add servers to My Servers (similar to a shopping cart on an e-commerce site). Using My Servers allows you to view and perform actions on selected servers.

When you use the same browser and login to the SAS Web Client running in the same facility, servers stay in My Servers for one year or until you explicitly remove them. Each time that you login to the SAS Web Client, you see the servers that were in My Servers the last time that you logged in.

The My Servers feature is available only on a per-user basis. You cannot log in as an Opware administrator to see the servers in the My Servers area of other Opware users.

Adding Servers to My Servers

Perform the following steps to add a server to My Servers:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the servers that you want to add to the My Servers.

Or


Search for the servers that you want to add to My Servers.

See “Using the Search Feature” on page 243 in this chapter for more information.
See “Server Searching by IP Address” on page 258 in this chapter for more information.

- 2** Select the servers that you want to add to My Servers.
- 3** Choose **Resource ► Add to My Servers** from the menu above the Manage Servers list. The Add To My Servers window appears, which indicates that you added the chosen number of servers to My Servers.
- 4** Click **Close** to close the window.
- 5** Next, select the My Servers link at the top of the page. You see the selected servers added to My Servers, as Figure 7-6 shows.

Figure 7-6: Servers in My Servers

My Servers (Summary View) ?

Resource Edit View Tasks Configuration Tracking							
<input type="checkbox"/>	Name ▲	Host Name / IP Address	OS Version	Stage	Use	Facility	Customer
<input type="checkbox"/>	 m098.dev.opsware.com	m098.dev.opsware.com 192.168.192.67	SunOS 5.8	Not Specified	Production	C03	Opware

You can perform the same server management tasks on servers in My Servers as on the servers in the Manage Servers list.

Removing Servers from My Servers

Perform the following steps to remove servers from My Servers:

- 1** Click the My Servers link in the navigation panel of the SAS Web Client. The My Servers page appears that shows the servers currently added to it.
- 2** Select the servers that you want to remove from My Servers and choose **Edit ► Remove from My Servers** from the menu above the Server list.

The My Servers page refreshes and displays the remaining servers in My Servers.

Server Search

This section provides information about Server Search and contains the following topics:

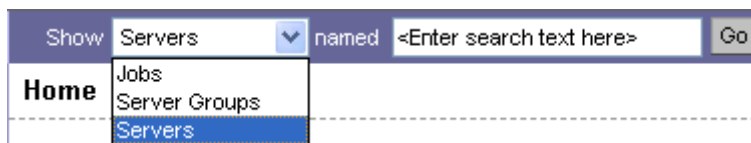
- Searching for a Server By Using the Search Box
- Ways to Use Search
- Using the Search Feature
- Rules for Server Search and for Creating Dynamic Groups
- Line Break Workaround for Server Search
- Conditions for Searching with Multiple Rules
- Server Searching by IP Address
- Example: Server Search
- Searching for a Server Group

Searching for a Server By Using the Search Box

Perform the following steps to search for a server using the Search box:

- 1** On the Home page, click the down arrow in the top navigation panel to open the Search box, as Figure 7-7 shows.

Figure 7-7: Search Text Box on the SAS Web Client Home Page



- 2** Verify that the Servers option is selected in the list.
- 3** Type the server's IP address, host name, or name in the Search box and then click **Go**.

The search text that you enter can include an asterisk (*) wildcard character. However, the search feature automatically prepends and appends an asterisk to the text.

For example, you can type any of the following search queries:

```
192.168.68.6
host02.coredev-va1.sample.com
192.168.*.19
```

host1*.xyz.samplecompany.com

The resulting page contains one or more servers, depending on the type of search query that you specified. If no servers are found, the SAS Web Client displays a message that indicates that no servers were found that matched your query.

See “Using the Search Feature” on page 243 in this chapter for information about how to formulate complex, multiple rule search queries.

Ways to Use Search

By using the SAS Web Client, you can perform searches in the following ways:

- From Opsware wizards

While using the Opsware wizards from the Tasks panel, you are prompted to select (by browsing or searching) servers or server groups, and operating systems, at specific points in the process.

What you can search for in the Opsware wizards is context sensitive to the type of operation that you are performing.

- From the navigation panel, click Servers ► Search.

The Search page allows you to search for managed servers that match specified rules.

- While adding or modifying rules for a dynamic group (By clicking **Search** on the Rules tab for a group).

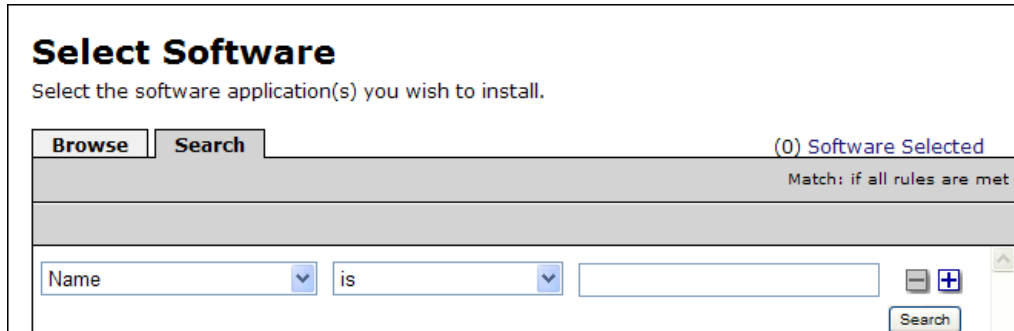
Using the Search Feature

In the Opsware wizards, you can browse for servers, operating systems, or use the Search feature to search for these items.

Perform the following steps to search by using the Search feature:

- 1 In an Opware wizard, select the Search tab. The following Search page appears. See Figure 7-8.

Figure 7-8: Search Tab in the Select Servers Step of an Opware Wizard

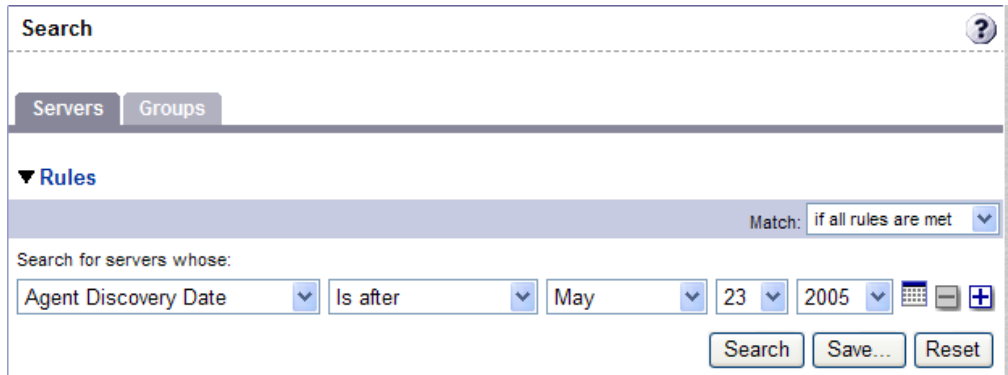


You can also use the Search tab at other steps in the wizards to search for operating systems, patches, applications, and templates.

Or

From the navigation panel, click Servers ► Search. The Search page appears, as Figure 7-9 shows.

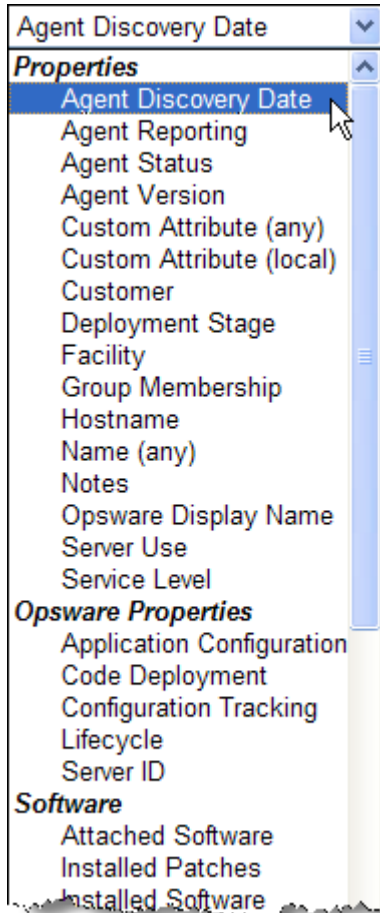
Figure 7-9: Search Page



By default, one search rule is added to the search.

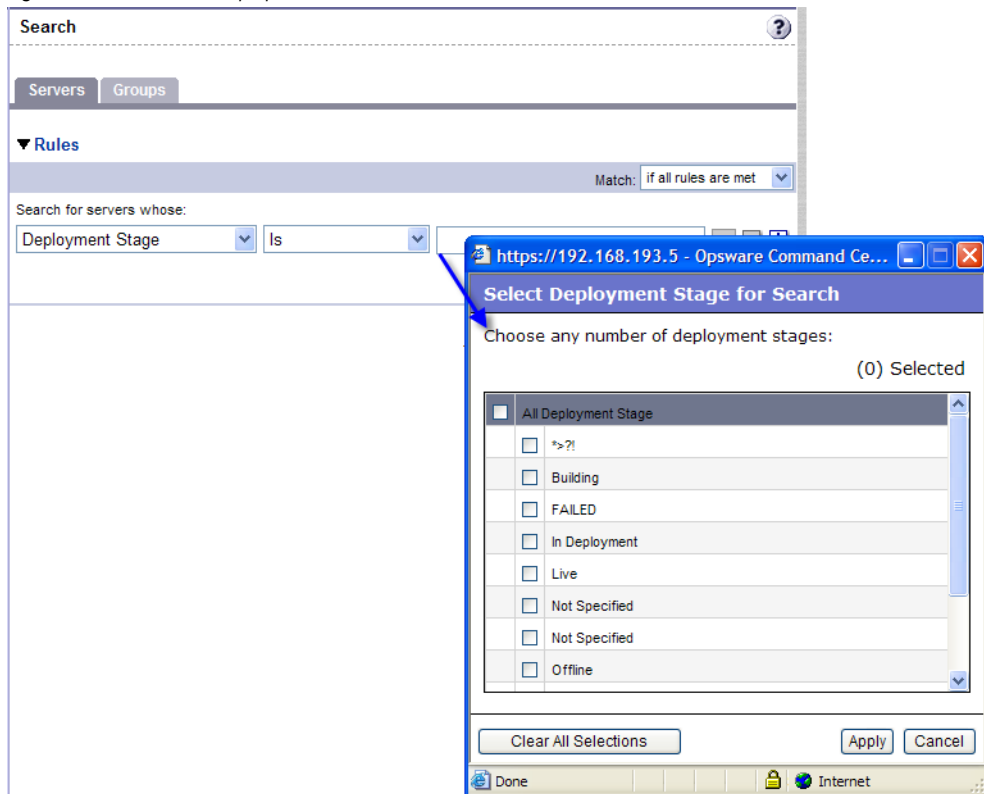
- Specify the rule that you want to search for by selecting it from the first list, as Figure 7-10 shows.

Figure 7-10: Search Rules List in the Search Page



Depending on the rule that you select, a popup window might appear in the page. For example, if you selected Deployment Stage, a popup window showing the stages appears in the page as Figure 7-11 shows:

Figure 7-11: Search Popup Window with Values



You cannot search in Notes that contain line breaks. See “Line Break Workaround for Server Search” on page 257 in this chapter for more information and a workaround.

If you are searching while using an Opsware wizard, the first search rule list might not have all the options. The list only includes the options that are relevant for the Opsware wizard that is being used. For example, the Install OS Wizard does not include options to search for installed patches on the servers.

- 3** In the second list, specify how you want Opsware SAS to search by selecting a value. The operator selected defines how the search text is treated. Negative operators might not be available in all cases.

See “Rules for Server Search and for Creating Dynamic Groups” on page 248 in this chapter for more information about the operator for each search rule.

- 4 Enter the text that you want to search for in the text box or choose a value from the list or popup window. The search text that you enter can include an asterisk (*) wildcard character. The search text is case insensitive. You can also use the SHIFT or CTRL key to select multiple values from the list or popup window.
- 5 (Optional) To add additional rules, click the plus (+) button as Figure 7-12 shows and repeat Steps 2 through 4.

Figure 7-12: Multiple Rules in a Search

The screenshot shows a search interface with the following elements:

- Search** header with a help icon.
- Tabs for **Servers** and **Groups**.
- Rules** section with a dropdown menu.
- Match:** dropdown menu set to "if all rules are met".
- Search criteria: "Search for servers whose:"
- Rule 1: Deployment Stage (dropdown) is (operator) In Deployment (text box).
- Rule 2: Opware Display Name (dropdown) Contains (operator) marketing (text box).
- Buttons: Search, Save..., and Reset.

- 6 If you specified multiple rules for the search, select whether you want search results only if all rules are met or if any of the rules are met, as Figure 7-13 shows.

Figure 7-13: Operator Controlling Search Results

The close-up shows the **Match:** dropdown menu with the following options:

- if all rules are met (selected)
- if any rules are met

By default, search results appear for servers that match all the search rules. If you are searching from an Opware wizard, this field is set to the value if all rules are met; you can change the value when searching for servers, but you cannot change it when searching for patches, software, operating systems, and so on.

- 7** Click **Search**. The list of servers that match your search rules appears in the page, as Figure 7-14 shows.

Figure 7-14: Displayed Search Results

Results						
Resource Edit Tasks Configuration Tracking						
<input type="checkbox"/>	Name ^	Host Name	IP Address	OS Version	Facility	Customer
<input type="checkbox"/>	 casela.snv1.corp.opsware.com Web Services test box	casela.snv1.corp.opsware.com	192.168.9.191	SunOS 5.9	C12	Opware
<input type="checkbox"/>	 chamarel.snv1.corp.opsware.com Web Services test box	chamarel.snv1.corp.opsware.com	192.168.9.146	Red Hat Linux 7.3	C12	Opware

The search results include columns for Name, IP Address, OS Version, Facility, and Customer.

When you search for installed software or patches and include an asterisk in the search text, Opware SAS might take several minutes to display the search results.

Rules for Server Search and for Creating Dynamic Groups

The following table describes the rules that you can use to search for servers or to create dynamic server groups.

Note that anywhere you can enter text, you can enter a wildcard (*) character to broaden your results.

Table 7-3: Rules for Server Search and for Creating Dynamic Groups

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
PROPERTIES		
Agent Discovery Date: The date that the Opware Agent was installed.	<ul style="list-style-type: none"> • Is after • Is before 	Drop-down lists with the day, month, and year
	<ul style="list-style-type: none"> • Is within the last 	User-entered text
	<ul style="list-style-type: none"> • Is today 	N/A

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
Agent Reporting: Whether the Opware Agent is reporting to Opware SAS.	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • Has not reported • OK • Registration in progress • Reporting error
Agent Status: Whether the Opware Agent is reachable by Opware SAS.	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • Not reachable • OK
Agent Version: The version of the Opware Agent – such as 14.2.3b.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
Custom Attribute (any): The name of a custom attribute that is associated with the server through attachment or inheritance.	<ul style="list-style-type: none"> • Contains • Is 	User-entered text
Custom Attribute (local): The name of a custom attribute that is locally attached to the server,	<ul style="list-style-type: none"> • Contains • Is 	User-entered text
Customer: The customer or account that the server is associated with.	<ul style="list-style-type: none"> • Is • Is not 	Popup window of customers

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Deployment Stage: The stage the server performs within a lifecycle environment.</p>	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • In Deployment • Live • Not Specified • Offline <hr/> <p>The values that appear in this list are customizable; in addition to the values above, values specific to your environment might appear.</p>
<p>Facility: The collection of servers managed by an Opware SAS installation.</p>	<ul style="list-style-type: none"> • Is • Is not 	<p>Popup window of facilities</p> <hr/> <p>When Opware SAS is running multimaster mode, the list can contain many facilities.</p>
<p>Group Membership: Whether the server belongs to a group.</p>	<ul style="list-style-type: none"> • Is 	<p>Popup window of groups</p>
<p>Host name: The host name of the server – such as m004.company.com.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Name (any): This enables searching for any name or IP address associated with a server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Notes: The contents of the Notes field from the Properties tab for a server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Opware Display Name: The user-configurable name for the server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p> <hr/> <p>By default, Opware SAS uses the configured host name of the server until a user edits it.</p> <hr/>
<p>Server Use: How the server is being used – such as Development, Staging, Production.</p>	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • Development • Not Specified • Production • Staging <hr/> <p>You can customize values that appear in this list. In addition to the values above, values specific to your environment might appear.</p> <hr/>
<p>Service Level: The user-defined category that can be used as an organizational tool.</p>	<ul style="list-style-type: none"> • Is • Is attached here or below 	<p>Popup window of service levels</p> <hr/> <p>Servers can be associated with multiple service levels.</p> <hr/>
<p>OPSWARE PROPERTIES</p>		

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Application Configuration: Whether the server uses the Application Configuration feature.</p>	<ul style="list-style-type: none"> • Is not used • Is used 	N/A
<p>Code Deployment: Whether the server uses the Code Deployment feature.</p>	<ul style="list-style-type: none"> • Is not used • Is used 	N/A
<p>Configuration Tracking: Whether the Configuration Tracking feature is monitoring or backing up specific files or configurations on a server.</p>	<ul style="list-style-type: none"> • Is off • Is on 	N/A
<p>Lifecycle: The server states that are part of bringing a server into Opware SAS.</p>	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • Available • Build Failed • Deactivated • Installing OS • Managed
<p>Server ID: The internal ID Opware SAS uses to identify the server.</p>	<ul style="list-style-type: none"> • Is • Is not 	<p>User-entered text</p> <hr/> <p>In most cases, the Server ID is the same as the MID.</p> <hr/>
SOFTWARE		
<p>Attached Software: The software that is assigned or modeled through the Opware installation process.</p>	<ul style="list-style-type: none"> • Is • Is attached here or below 	<p>Popup window of software</p>

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Attached Software Policies: The software policies that is assigned or modeled through the Opware installation process.</p>	<ul style="list-style-type: none"> • is 	<p>Popup window of software policies</p>
<p>Installed Patches: Whether a patch is installed on the server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Installed Software: The package reported installed on the server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p> <hr/> <p>A package does not have to be installed by Opware SAS to be reported as installed on a server.</p> <hr/>
<p>OS Version: The OS version defined by OS definitions in the OS Provisioning feature.</p>	<ul style="list-style-type: none"> • Is • Is not 	<p>Popup window of operating systems</p>
<p>Reported OS: For Windows – the version reported by the OS, for Unix – the version returned by the uname command.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Windows Service: The names of the Windows services that are reported to Opware SAS.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>NETWORK</p>		

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
DNS Search Domains: The domains configured to be searched in the server's network settings.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
DNS Servers: The IP addresses of the DNS servers configured in the server's network settings.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
Default Gateway: The IP address of the default router.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
IP Address: Any Internet Protocol address for the server.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
MAC Address: Any Media Access Control address, which is the network interface card's unique hardware number.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
WINS Servers: The Windows Internet Naming Servers configured in the server's network settings.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
HARDWARE		

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
CPU Make and Model: The vendor name and CPU model for the server – such as GENUINEINTEL Intel(R) Pentium(R) 4 CPU 2.60GHz.	<ul style="list-style-type: none"> • Is • Is not 	Popup window of CPU makes and models
CPU Speed: The Central Processing Unit speed in gigahertz [GHz].	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text <hr/> A 600 Mhz machine should be entered as 0.6. <hr/>
Make and Model: The vendor name and server model for the server – such as Compaq - DL360.	<ul style="list-style-type: none"> • Is • Is not 	Popup window of server makes and models
Number of CPUs: The number of CPUs on the server.	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text
RAM: The amount of RAM on the server in megabytes [MB].	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text <hr/> To enter 1 Gigabyte, type 1024. <hr/>
Serial Number: The serial number of the server.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text

Table 7-3: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Storage Make and Model: The vendor name and storage model for the server – such as WDC - WD800BB-75DKA0.</p>	<ul style="list-style-type: none"> • Is • Is not 	<p>Popup window of storage makes and models</p>
CUSTOM FIELDS		
<p>A Numeric field</p>	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	<p>User-entered text</p>
<p>A String field</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>A URI field</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>A File field</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>A Date field</p>	<ul style="list-style-type: none"> • Is after • Is before 	<p>Drop-down lists with the day, month, and year</p>
	<ul style="list-style-type: none"> • Is within the last 	<p>User-entered text</p>
	<ul style="list-style-type: none"> • Is today 	<p>N/A</p>

Line Break Workaround for Server Search

You cannot search in notes that contain line breaks. For example, you cannot search for text in a note when it is this type of text:

```
line1 <line break>
```

```
line2
```

For example, the following query does not return any results:

```
Any/all notes contain line1 <line break> line2
```

However, the following query does return all servers that have notes:

```
Any/all notes is not line1 <line break> line2
```

To work around this limitation, include an asterisk (*) where the line break occurs, as Figure 7-15 shows. For example:

```
Any/all notes is line1*line2
```

Figure 7-15: Line Break Workaround in the Server Search Feature

The screenshot shows the 'Search' interface in the SAS Web Client. At the top, there are tabs for 'Servers' and 'Groups'. Below the tabs, there is a 'Rules' section with a dropdown arrow. A 'Match:' dropdown is set to 'if all rules are met'. The main search area is titled 'Search for servers whose:' and contains a dropdown menu set to 'Notes'. To the right of this dropdown is another dropdown set to 'Is'. The search query 'line1*line2' is entered in the text input field. To the right of the input field are three small icons: a plus sign, a minus sign, and a plus sign. Below the input field are three buttons: 'Search', 'Save...', and 'Reset'.

Conditions for Searching with Multiple Rules

When you perform a search with multiple rules, the following conditions apply to the way Opware SAS provides search results:

- When it evaluates rules, the Search feature considers each rule individually, finding servers (or operating systems, patches, and so forth) that match the individual rule, and then the results of each rule are combined.
- You must select at least one rule, and it must have a value. Default filter rules count as rules with a value.

- Empty rules are ignored in searches. Users do not have to manually remove them for the search to proceed.
- You cannot search for empty values. For example, you cannot search for all servers where the Notes field is empty.

At certain steps in the Opware wizards, the Search feature provides default values based on previous selections in the wizard.



The wizards are flexible; for example, when you select multiple servers and applications, Opware SAS will install the correct applications on the servers, even if you selected different OS versions for the servers and applications in the respective steps. Opware SAS also matches the customer association for applications, operating systems, and templates with the customer association of servers.

If Opware SAS cannot find a match, an error message appears at the end of the wizard; therefore, use caution when modifying these default values.

Server Searching by IP Address

Users can search for servers by entering a specific IP address in the Search box in the top navigation or in the Search feature.

Opware SAS includes support for static Network Address Translation (NAT). This feature introduces the concept of a management IP, which might be different from any of the local IP addresses that the Opware Agent reported for a server.

When searching for a server based on its IP address, the Search feature searches based on the server's primary IP address and based on the IP address for any interface that server has, including its management IP address. In the search results, an extra column is shown that lists all matching IP addresses for all interfaces. The management IP address is included if the server's networking is configured for static NAT.

See "Communication Between Managed Servers and Opware SAS" on page 275 in Chapter 8 for information about how Opware SAS handles servers that are affected by static NAT.

Example: Server Search

Using the Search feature, a user creates a query with the following conditions:

- Installed Software contains qa

- Installed Software contains man
- If all rules are met is selected

The results of this search will be all servers that have at least one installed package with qa somewhere in its name and at least one installed package (not necessarily the same one) with man in its name.

The search results are not limited to packages that contain both qa and man in the package name.

Find all servers that have some version of Apache or some version of Java installed:

- Installed Package contains apache
- Installed Package contains java
- If any rules are met is selected

Searching for a Server Group

- 1 From the navigation panel, click Servers ► Search. The Search page appears. By default, the Servers tab is selected.

Select the Groups tab. The rules for server group search appear as Figure 7-16 shows. By default, one search rule is added to the search.

Figure 7-16: Rules for Server Group Search

The screenshot shows the 'Search' interface with the 'Groups' tab active. Under the 'Rules' section, there is a 'Match:' dropdown set to 'if all rules are met'. Below this, the text 'Search for groups whose:' is followed by a dropdown menu set to 'Group Name', an operator dropdown set to 'Contains', and an empty text input field. To the right of the input field are three small icons: a plus sign, a minus sign, and a square. A 'Search' button is located at the bottom right. A dropdown menu is open under the 'Group Name' dropdown, showing 'Properties' and 'Group Name' as options.

- 2 In the second list, specify how you want Opware SAS to search by selecting either “Contains” or “Is”. The operator selected defines how the search text is treated.
- 3 Enter the text that you want to search for in the text box. The search text that you enter can include an asterisk (*) wildcard character. (The search text is case sensitive. **Search** is not enabled until you enter text in the text box.)



When searching for a server group, you can only specify one rule for Group Name. The plus (+) button is disabled.

4 Click **Search**. The search results appear as Figure 7-17 shows.

Figure 7-17: Server Group Search Results

The screenshot shows the 'Search' interface in Opware SAS. It has tabs for 'Servers' and 'Groups', with 'Groups' selected. Under the 'Rules' section, there is a search filter set to 'Group Name' containing 'test'. The 'Results' section shows a table with one entry: 'a test group'.

	Name ^	Location	Members		Total Servers	Type	Model Attachments	Custom Attributes	Last Use
			Servers	Subgroups					
<input type="checkbox"/>	a test group	Public Groups	0	0	0	Dynamic	3	0	05-22-05 16:00:00

Server Identification

This section provides information on server identification within Opware SAS and contains the following topics:

- Overview of Server Identification
- Ways that Servers are Identified by Opware SAS
- Customer Accounts in Opware SAS
- Associating Servers with Customers

Overview of Server Identification

Opware SAS uses the following IDs to track managed servers:

- **MID:** Machine ID. The unique identifier that Opware SAS uses to identify the server. The MID is usually equal to the server ID.

The MID is stored in a file on a server's disk so that the MID can persist and be read by the Opsware Agent.

The MID follows the hard disk, not the chassis, so system administrators can swap chassis for servers without affecting how Opsware SAS tracks those servers.

See "Example: Opsware SAS Swaps a Server's Hard Disk" on page 262 in this chapter for information about swapping hard disks.

- **Server ID:** The primary key in the Opsware Model Repository (database) that represents a given server. The Server ID is used internally in Opsware SAS. Generally, users do not need this value for servers to manage them in Opsware SAS.
- **MAC Address:** Media Access Control address, which is the network interface card's unique hardware number. The MAC is used as the server's physical address on the network.
- **Chassis ID:** A unique hardware-based identifier that the Opsware Agent discovers, typically derived from some property of the server's chassis. As a common source for this ID, Opsware SAS uses an interface's MAC address or the host ID on Solaris servers, or the serial number for one of the interfaces.

Ways that Servers are Identified by Opsware SAS

Servers in the Manage Servers list are identified in the following ways when they register their hardware and software with Opsware SAS:

- Opsware SAS identifies each server by using the MID first.
- If the MID cannot be determined, the chassis ID is used to identify the server.
- If the server cannot be identified with the chassis ID, the MAC addresses are used to identify the server.

In the Server Pool, the MAC Address column displays values by which Opsware SAS tracks the servers. The value used varies by platform:

- Intel x86 processor-based servers are identified by the MAC address of the server.
- Sun SPARC processor servers are identified by the host ID of the server.

The host ID for Sun SPARC processor servers appears in the MAC Address column in the Server Pool list.

To determine the value in the MAC Address column, Opware SAS uses the hardware address by which the server contacted the Opware Build Manager (a component of the OS Provisioning feature).

Example: Opware SAS Swaps a Server's Hard Disk

The following steps show how Opware SAS handles swapping a hard disk for a server:

- 1** A system administrator swaps the hard disk of Server A (MID 1230001, chassis ID AB:08) with the hard disk of Server B (MID 98730001, chassis ID XY:96).
- 2** The Opware Agent on Server A registers its hardware with Opware SAS. The MID for Server A equals 1230001 and the chassis ID equals XY:96.
- 3** Opware SAS locates Server A by using the MID.
- 4** Opware SAS updates the data it has for Server A in the Model Repository. It sets the chassis ID equal to XY:96.
- 5** The Opware Agent on Server B registers its hardware with Opware SAS. The MID for Server B equals 98730001 and the chassis ID equals AB:08.
- 6** Opware SAS locates Server B by using the MID.
- 7** Opware SAS updates the data it has for Server B in the Model Repository. It sets the chassis ID equal to AB:08.


Customer Accounts in Opware SAS

Many enterprise customers have consolidated disparate IT operations into a single operation, yet they still need separate reporting, billing, and management for different business units or groups (for example, West Coast Office, East Coast Office, and London Office).




Opware SAS accommodates these requirements with customer accounts created by your Opware administrator.

When your Opware administrator creates a customer in Opware SAS, a value for that customer is automatically added to the customer filter in the Manage Servers list, as Figure 7-18 shows.

Figure 7-18: Customer Filter in the Manage Servers List

Manage Servers (Summary View) 

All Statuses All Operating Systems All Stages
 All Uses All Customers All Manufacturers
 All Models All Customers MYCUSTOMER Not Assigned Configuration Tracking

<input type="checkbox"/>	Name	Host Name / IP Address	OS Version	Stage	Use	Customer
 Public Groups						
<input type="checkbox"/>	 core.tr3.opsware.com	core.tr3.opsware.com 172.16.36.18	Red Hat Enterprise Linux AS 3	Not Specified	Not Specified	Opware
<input type="checkbox"/>	 OPSWARE-STROCOZ	OPSWARE-STROCOZ 172.16.36.43	Windows 2000	Not Specified	Not Specified	Not Assigned

By using customer accounts in the SAS Web Client, you can segregate servers that belong to different business units. By segregating servers, you can have separate accounting for each customer or different levels of security for different customers. You might want to segregate the servers based on the department or business unit.

By default, Opware SAS is shipped with the following two customers:

- **Customer Independent:** A global customer in Opware SAS. Resources that are associated with “Customer Independent” can be installed on any managed server, no matter what customer it is associated with.
- **Not Assigned:** The servers are not associated with a customer. You can install resources that are Customer Independent on Not Assigned servers. However, you cannot install or use any resources associated with a customer on a server that is not assigned to a customer.

When you install an Opware Agent in a server, the server is associated with the Not Assigned customer if IP ranges were not created to automatically associate Opware SAS managed servers with customers. See Figure 7-19.



Opware, Inc. recommends that you associate servers with customers, if necessary, by using the Server Properties pages.

Figure 7-19: Customers List Under Environment in the SAS Web Client

Customers			
	Name		Name
	12204		Corp Test
	Big Corp		Big Corp2
	Test Cust		Customer Independent
	E-Commerce		Not Assigned

Associating Servers with Customers

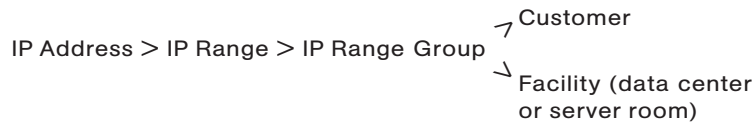
An Opware user or an Opware administrator can set up an IP range group so that servers are automatically associated with customers when users perform the following server management tasks:

- Install Opware Agents on the servers.
See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for more information.
- Use the OS Provisioning feature to install operating systems on bare-metal servers.
See *Opware® SAS User's Guide: Application Automation* for more information.

To set up this automatic customer association, you must create IP range groups for customers and specify the ranges of IP addresses that the groups contain.

In the SAS Web Client, an IP range group is both a physical and logical list – an accounting way to group ranges of IP address and assign them to a particular customer. An IP range identifies a range of IP addresses within an IP range group.

When you set this up, IP addresses get their customer association through the IP range, which, in turn, gets its customer association from the IP range group.



See the *Opware[®] SAS Policy Setter's Guide* for more information.

The loose relationship between server and IP address means that you can associate a server with a different customer from its IP address.

Even when IP range groups are set up for a customer, a server's IP address does not necessarily determine the customer to which the server is associated because a user can change the customer association in the Server Properties page.

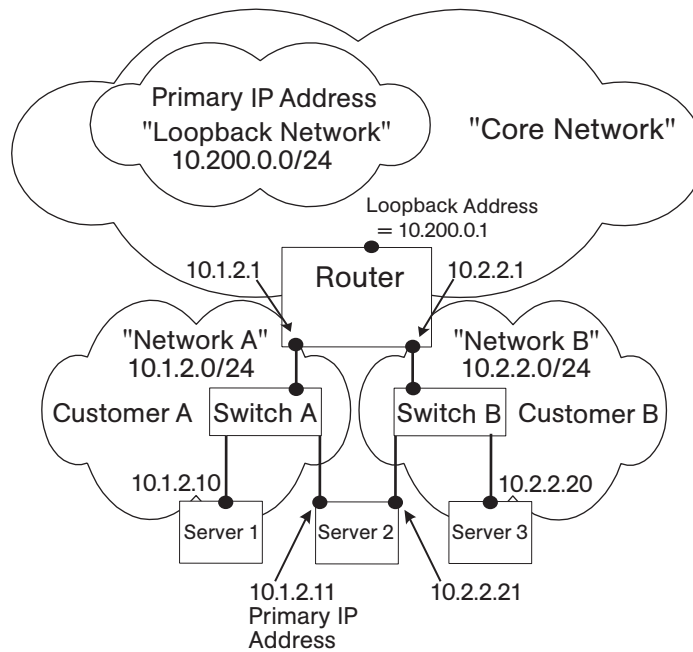
See “Editing the Properties of a Server” on page 320 in Chapter 8 for information about how to change the customer association for a server.

The customer association for a server is based on the management IP address of the server and not the primary IP address.

See “Communication Between Managed Servers and Opware SAS” on page 275 in Chapter 8 for information about how Opware SAS uses management IP addresses for servers.

However, a server always belongs to the same facility (data center or server room) as its primary IP address. Opsware SAS enforces the relationship between server and facility at hardware registration. See Figure 7-20.

Figure 7-20: Primary IP Addresses in Opsware SAS



In this illustration, the following conditions apply:

- Server 1 belongs to Customer A.
- Server 2 belongs to Customer A but has IP addresses in Network A and Network B.
- Server 3 belongs to Customer B.
- The Router belongs to the Core Network but has IP addresses in Network A and Network B.

Server Histories and Reports

This section provides information on server histories and reporting with Opware SAS and contains the following topics:

- Overview of Server History
- Viewing Server History
- Time Stamp for Server Operations

Overview of Server History

By using the SAS Web Client, you can view the history of changes made to a server. Each action performed on a managed server is logged in the history with the associated user who performed the action and the time of the action. You can view the history at any time, but you cannot change it. History is read-only.

Each History entry contains three pieces of information, as Table 7-4 shows.

Table 7-4: 'Description of the Entries in the Server History Tab

HISTORY ENTRY	DESCRIPTION
Event Description	Description of the operation performed, for example: Run ISM Control: ad-hoc script (Job ID: 26190040) executed successfully.
Modified By	The name of the Opware user who made the change.
Date Modified	The date and time the change was made, for example: Mon Aug 06 18:14:41 GMT+00:00 2001)

Time Stamps used in History

Data is maintained for servers in Opware SAS for the following periods of time:

- The SAS Web Client maintains the history of changes for the last three-month interval.
- Command Engine session logs are retained for 30 days, except for the last remediate session for a server, which is retained indefinitely.

The Command Engine is the Opware SAS component that enables distributed programs to run across many servers.

- Server history is retained for 6 months.



If longer periods of time are required, Opware, Inc. recommends regular backups to enable offline storage of Opware SAS data.

Opware SAS deletes old data from the Opware Model Repository, and does not copy the data before it removes it, but you can retain information for longer periods of time, by using Oracle commands to manipulate scheduled jobs. Contact your Opware, Inc. support representative for assistance in changing these retention periods.

Viewing Server History

Perform the following steps to view the server history:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server whose history you want to view.

Or

Search for the server whose history you want to view.

See “Using the Search Feature” on page 243 in this chapter for more information.

See “Server Searching by IP Address” on page 258 in this chapter for more information.

2 Click the name of the server whose information you want to see. The Manage Servers: Properties page appears for that server.

3 Select the History tab.

By default, the view shows changes made within the past week.

Time Stamp for Server Operations

Opware SAS maintains a comprehensive audit trail of the software that the Opware users install, configure, and remove from a server. By using the SAS Web Client, you can view the history of the changes made to a server. Entries are generated when actions are performed for managed servers in the SAS Web Client. The history is read-only. See “Server Histories and Reports” on page 267 in this chapter for more information.

The time stamps for system events are determined based on the system clocks of the servers running the Opware core components. To obtain accurate time stamps in server histories (displayed in the SAS Web Client) and Opware component logs, you must:

- Synchronize the system clocks on all servers running Opware components so that all the servers are running with a common time.
- Set the time zone for all servers running Opware components to Coordinated Universal Time (UTC).

See the *Opware[®] SAS Planning and Installation Guide* for more information on facility time requirements.

Additionally, Opware, Inc. recommends that after installing an Opware Agent on the server (so that it becomes managed by Opware SAS), you should synchronize the system clock on the server with the system clocks of the servers running the Opware core components.

The time stamps appearing in the SAS Web Client server History tab and the Opware Agent logs are obtained from the Opware core; however, you might need to review the server’s logs (such as, stdout). Having a consistent time stamp in the server’s logs and Opware SAS is essential for effective troubleshooting.

Hardware Information for Managed Servers

The Hardware link of the SAS Web Client provides a read-only view of all servers in your managed environment categorized by hardware manufacturer and model. The Hardware link provides hardware related information for each server, such as:

- Manufacturer
- Model number
- MAC ID
- Serial number
- CPUs used on the server
- Memory
- Storage capacity

See “Server Information that the Opware Agent Tracks” on page 103 in Chapter 4 for more information.

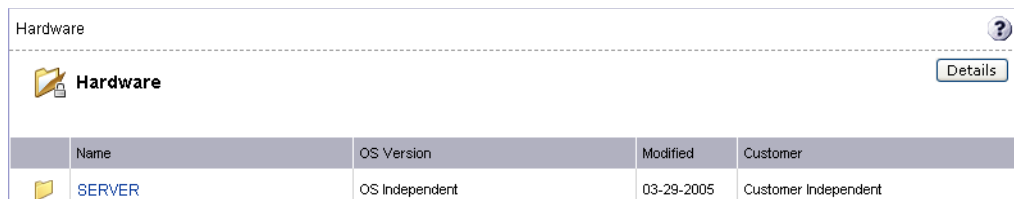
Viewing Managed Server Hardware Information


Viewing hardware information allows you to see all the servers in your managed environment by hardware vendor, and view such information as MAC ID, CPUs, memory, and so on.

To view hardware of managed servers:

- 1 From the navigation panel, click Environment ► Hardware. You see the top level of the Hardware category in the managed environment, as shown in Figure 7-21.

Figure 7-21: Top level hardware



	Name	OS Version	Modified	Customer
	SERVER	OS Independent	03-29-2005	Customer Independent

- 2 To view the servers in your managed environment, click the Servers link.

- 3 Drill down to the type of server you want to look at. For example, you might want to look at all Dell POWEREDGE 650s, as shown in Figure 7-22.

Figure 7-22: Hardware home page for Dell POWEREDGE 650s

[Hardware](#) > [SERVER](#) > [DELL COMPUTER CORPORATION](#) > POWEREDGE 650



No Sub-Nodes

Properties	Members 107
Cannot edit or delete this Node. This Node is auto-generated. This Node is special and cannot be modified.	
Name:	POWEREDGE 650
Customer:	Customer Independent
Operating System:	OS Independent
Locked:	No
Allow Servers:	Yes
ID:	1960003

- 4 Next, select the Members tab. You will see a list of all the Dell POWEREDGE 650s in your managed environment.
- 5 To view specific hardware information, from the **View** menu, choose **Hardware**. You now see more detailed information about all the Dell POWEREDGE 650s computers being managed by Opware SAS.

Chapter 8: Server Management in SAS Web Client

IN THIS CHAPTER

This section discusses the following topics:

- Overview of Server Management
- Communication Between Managed Servers and Opsware SAS
- Server Groups
- Server Life Cycle
- Server Management Jobs
- Custom Fields for Servers
- Custom Attributes for Servers
- Network Configuration

This section does not document how to install operating systems, patches, or applications on servers. However, it does discuss how those tasks fit into the overall server life cycle, and it does provide cross-references to the appropriate topics in other sections.

Overview of Server Management

Opsware SAS manages servers in an operational environment in the following ways:

- Provisioning servers with Microsoft Windows, Red Hat Linux, and Sun Solaris operating systems by using vendor-provided operating system bootstrapping technologies. Additionally, Opsware SAS integrates with AIX NIM and HP-UX Ignite installation technologies to provide a uniform method for OS provisioning across a heterogeneous environment.

See *Opware® SAS User's Guide: Application Automation* for information about how Opware SAS provisions Microsoft Windows, Red Hat Linux, Sun Solaris, and VMware ESX operating systems on managed servers.

See the *Opware® SAS Administration Guide* for information about how Opware SAS integrates with AIX NIM and HP-UX Ignite installation technologies.

- Providing configuration tracking, which allows users to monitor selected configuration files and databases and to take certain actions when change is detected.

See "Configuration Tracking" on page 463 in Chapter 13 for more information.

- Automating the management and execution of server scripts.

See See "Distributed Script Execution" on page 399 in Chapter 11 for more information.



To manage servers with Opware SAS, you do not need root access on Unix or administrator access on Windows. However, you will need permissions to use specific Opware SAS features, as well as permissions for customers and facilities associated with servers. To obtain these permissions, contact your Opware administrator. For more information, see the Permissions Reference appendix in the *Opware® SAS Administration Guide*.

Communication Between Managed Servers and Opware SAS

This section provides information about communication between managed servers and Opware SAS and contains the following topics:

- Network Address Translation (NAT) for Managed Servers
- Key Terms of Opware SAS Managed Server Communication
- Locating the Management IP Address of a Managed Server
- Code Deployment and Static NAT
- Setting the Primary IP Address of a Server
- NAT Table Mapping and Managed Servers

Network Address Translation (NAT) for Managed Servers

To manage a server, Opware SAS requires that the server have a unique IP address that is routable from Opware SAS. However, in a large operational environment, all servers might not have unique IP addresses. In this case, Opware SAS supports static Network Address Translation (NAT) for managed servers.

Static NAT maps public IP addresses to hosts inside the internal network, which allows Opware SAS to manage all servers in the environment.

Unlike dynamic NAT, the mapping between Opware SAS and the servers under management is set ahead of time, not dynamically at runtime.

Key Terms of Opware SAS Managed Server Communication

To understand how Opware SAS communicates with managed servers, you must understand these three terms:

- **Management IP:** The IP address that Opware SAS uses to communicate with the Opware Agent on the server.

During hardware registration for a server, the Opware Agent opens a TCP/IP connection to Opware SAS. The connection contains the source IP (called peer IP) address of the server. By default, Opware SAS uses this peer IP address as the management IP for the server.

- **Management Interface:** When a server has more than one network interface, you can designate one of them as the management interface.

- **Primary IP:** The IP address of the management interface. When you change the management interface, the primary IP changes to the IP address of that interface. The primary IP address is a locally-configured IP address.

During synchronizations, the Code Deployment & Rollback feature uses the primary IP address to communicate with the server. See “Code Deployment and Static NAT” on page 278 in this chapter for more information.

The Opware Agents on servers communicate with each other by using the primary IP addresses, even though Opware SAS uses management IP addresses to communicate with the servers.



Opware SAS does not support managed servers that have IPv6 addresses.

When static NAT is being used, the management IP address for a server will *not* be the same as the primary IP address. When static NAT is being used, the management IP is the NAT-translated IP address for the server. When static NAT is *not* being used, the management IP address is always the same as the primary IP address.

Locating the Management IP Address of a Managed Server

In the SAS Web Client, you can find the management IP address of a server and check whether it is using static NAT. You might need this information for troubleshooting any servers marked Not Reachable and to determine whether your NAT configuration is correct. The SAS Web Client displays the management IP address of a managed server in the following two places:

- The Network tab of the Server Details page
- The Hardware view of the Manage Servers list

The Network tab shows (and allows the user to set) the management interface for the server by selecting it from a drop-down list, as Figure 8-1 shows.

Figure 8-1: Management IP Address Information in the Network Tab

Properties	Network	Membership	Attached Nodes	Installed Packages	Custom Attributes	Config Tracking	History
NETWORK INFORMATION (as of Wed May 18 07:05:57 2005)							
Hostname:	<input type="text" value="core.tr3.opsware.com"/>						
Management IP:	172.16.36.18						
Facility:	DATACENTER1						
Management Interface:	<input type="text" value="eth0"/>						
Gateway:	<input type="text" value="172.16.36.17"/>						
DNS Servers:	<input type="text" value="66.54.32.78"/> <input type="text" value="66.54.0.78"/>						
Search Domains:	<input type="text" value="tr3.opsware.com"/> <input type="text" value="opsware.com"/>						
CONFIGURATION FOR: eth0							
Use DHCP Settings:	<input type="text" value="Static"/>						
IP Address:	<input type="text" value="172.16.36.18"/>						
MAC Address:	00:11:43:D7:2F:5F						
Interface Type:	ETHERNET						
Interface Speed:	(not set)						
Subnet Mask:	<input type="text" value="255.255.255.248"/>						
CONFIGURATION FOR: eth1							
Use DHCP Settings:	<input type="text" value="Disabled"/>						
IP Address:	<input type="text"/>						
MAC Address:	00:11:43:D7:2F:60						
Interface Type:	ETHERNET						
Interface Speed:	(not set)						
Subnet Mask:	<input type="text"/>						
<input type="button" value="Update"/> <input type="button" value="Revert"/>							

Figure 8-2 shows the Hardware view in the Manage Servers list, which displays the management interface for the server in the Network Info column. (To access the Hardware view, choose **Hardware** from the **View** menu.)

Figure 8-2: Hardware Tab in the Manage Servers List

Resource	Edit	View	Tasks	Configuration Tracking				
Name	Host Name / IP Address	Registration	Network Info	Hardware Info	Hardware Components			
Public Groups								
core.tr3.opsware.com	core.tr3.opsware.com 172.16.36.18	OK	172.16.36.18 (eth0) N/A (eth1)	Man: DELL COMPUTER CORPORATION Mod: POWEREDGE 1850 Mac: 00:11:43:D7:2F:5F Ser: 2YLLP61	CPUs: Intel(R) Xeon(TM) CPU 2.80GHz, 2793 MHz, 1 MB Intel(R) Xeon(TM) CPU 2.80GHz, 2793 MHz, 1 MB Intel(R) Xeon(TM) CPU 2.80GHz, 2793 MHz, 1 MB Intel(R) Xeon(TM) CPU 2.80GHz, 2793 MHz, 1 MB Memory: 3.9 GB RAM 1.95 GB SWAP Stor: hda (CDROM) sda (SCSI DISK:68.24 GB)			

The Network Info column shows the IP addresses and interfaces configured for each server in the list. If a server is using static NAT, the management IP is the first entry in this list and (NAT) appears after the IP address. If it is not using static NAT, the management IP is the same as the management interface, so it is already shown.

Code Deployment and Static NAT

Code Deployment and Rollback (CDR) synchronizations can only occur between Opware Agents in the same NAT domain. Synchronizations cannot be performed between Opware Agents in different NAT domains.

Opware SAS uses the primary IP address (instead of the management IP address) during synchronization because it is assumed that static NAT is not occurring between the servers in the synchronization. During CDR synchronizations, two Opware Agents must communicate directly. Users can override the IP address that Opware SAS determined and designate a specific network interface as the management interface.

See “Code Deployment and Rollback” on page 435 in Chapter 12 for information about how to use CDR.

Setting the Primary IP Address of a Server

When a server has more than one network interface, users can specify one of them as the management interface and the IP address for this interface is designated the primary IP address. The primary IP address is used for Opware Agent-to-Opware Agent communication.

If static NAT is *not* being used, the management and primary IP addresses are the same. If static NAT is being used, the management IP is unaffected when a user changes the management interface.

Perform the following steps to set the primary IP address of a server:

1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server whose management IP address you want to view.

Or

Search for the server whose management IP address you want to view.

2 Click the server name. The Manage Servers: Properties page appears.

3 Select the Network tab. The network information for the server appears.

The Network tab shows (and allows you to set) the server's management interface.

4 Set the management interface by selecting it from the Management Interface field. The IP address for this interface is designated the primary IP address.

5 Click **Update**.

See "Using the Search Feature" on page 243 in Chapter 7 for more information. See "Server Searching by IP Address" on page 258 in Chapter 7 for more information.

NAT Table Mapping and Managed Servers

Static, one-to-one NAT tables map routable IP addresses between Opware SAS and managed servers. Network administrators configure and maintain these NAT tables. After the static NAT tables are configured, you do not have to perform any additional setup for Opware SAS.

Opware SAS does not control these NAT tables and errors can occur if they are modified after Opware-managed servers register their hardware information. The following errors can occur if the IP address mapping of a server changes:

- If the IP address on the Opware SAS side of the NAT mapping is modified, the server becomes unmanageable and might be marked Not Reachable on the Manage Servers: Status page. It stays in this state until the Opware Agent requests another hardware registration and the server's management IP is updated.
- If an IP address mapped to a particular server is mapped to a different server, both servers become unmanageable and might be marked Not Reachable on the Manage

Servers: Status page. This problem is resolved when one of the two servers reports its IP address during hardware registration. The other server remains unmanageable until the server registers with the Opware Agent. Both servers eventually become manageable.

Server Groups

This section provides information on server groups within Opware SAS and discusses the following topics:

- Overview of Server Groups
- Types of Server Groups
- Public Group Modeling
- Ways to Create Server Groups
- Adding a Server to Static Groups, Both Public and Private
- Removing Servers from Static Groups, Both Public and Private
- Duplicating Server Groups
- Rules for Deleting Server Groups

Overview of Server Groups

The Server Groups feature is useful for gathering servers into collections. These groups can be used as a shortcut for performing the same action on all of the servers simultaneously, instead of performing the action on each individual server, one at a time. Server groups can also be used to simply organize groups of servers.

Server groups can be comprised of individual servers as well as other server groups.



The My Servers feature can also be used to gather servers and server groups, but it has different functionality than the Server Groups feature. You can add individual servers, server groups, and nested groups that you access frequently to My Servers. See “My Servers” on page 239 in Chapter 7 for information about using this feature.

Uses for Server Groups

Some recommended uses for server groups include:

- Grouping servers by OS version
- Grouping servers by customer
- Grouping servers by facility
- Grouping servers by deployment stage
- Grouping servers by use (Server Use in the Server Properties page)
- Grouping servers by operational boundaries, for example, grouping together all servers that require identical application configuration
- Grouping servers by access control boundaries, for example, creating server groups that are associated with a specific User Group

Permissions Required for Working with Server Groups

Users must have the permissions shown in Table 8-1 in order to perform specific tasks related to server groups. Only administrators can set permissions.

Table 8-1: Permissions Required for Working with Server Groups

NAME OF PERMISSION	WHERE SELECTED	ENABLES YOU TO
Manage Servers		Create, edit, and delete private server groups, both static and dynamic.
Manage Public Server Groups	The Manage Servers Permissions section on the Other tab in Users and Groups	Create, edit, and delete public server groups, both static and dynamic.
Model Public Server Groups	The Manage Servers Permissions section on the Other tab in Users and Groups	Model public server groups. See “Public Group Modeling” on page 284 in this chapter for more information.

Table 8-1: Permissions Required for Working with Server Groups (continued)

NAME OF PERMISSION	WHERE SELECTED	ENABLES YOU TO
Allow Run Refresh Jobs	The Manage Servers Permissions section on the Other tab in Users and Groups	Add or remove servers from groups before a scheduled job is run. This permission gives you the option to refresh group membership before a job is run so that it is only run on the servers that belong to the group when the job is actually run.

Characteristics of Server Groups

When using server groups, groups have the following characteristics:

- Individual servers can be included in as many groups as you want, or not included in any groups.
- Adding servers to a group does not remove those servers from the list of all servers that appears when you click Servers ► Manage Servers in the navigation panel.
- Groups can contain servers and subgroups.
- Server groups are hierarchical (they can be nested) with these caveats:
 - Private and public groups cannot be mixed in a hierarchy, but static and dynamic groups can.

See “Types of Server Groups” on page 283 in this chapter for more information about private and public groups.

- The rules for a dynamic group are not inherited from a parent dynamic group to a dynamic subgroup.

See “Dynamic Groups” on page 284 in this chapter for more information about the characteristics of dynamic groups.

- Groups do not inherit modeling data from their parents, including custom attributes.
- When you run an operation on a group that contains nested groups, the operation also applies to all the servers in the nested groups below the current group.

- When an Application Configuration operation within the SAS Client is applied to groups, and those groups contain subgroups, the operation does not apply to all the servers in the subgroups. It only applies to the group upon which the operation was directly applied.

Types of Server Groups

There are private groups and public groups, and each can be either static or dynamic.

Private Groups

If you belong to a user group that has access to the Manage Servers list, you can create groups that you alone can see and work with. Only you see your private groups – other Opware users cannot see them. Private groups behave the same way as public groups, with the exception that modeling is not available for private groups. See “Public Group Modeling” on page 284 in Chapter 8 for information about how the Opware model affects groups.

When you create your first group, the default type will be Private Static, which can be changed to Private Dynamic, Public Static, or Public Dynamic. When you create a subgroup, the type of group is private if you are in a private group when you create the new group, and the type is public if you are in a public group when you create the new group. Public and private groups cannot be mixed in a hierarchy. In other words, if the parent group is public, the subgroups must be public, and if the parent group is private, the subgroups are also private.

Public Groups

Public groups can be created, edited, or deleted by anybody who has Manage Public Server Groups permissions. Public groups are visible to all users, and can be used by anybody, regardless of who created them, but only users with the Manage Public Server Groups permissions can change the rules that govern dynamic groups.

A link called Public Groups appears at the top of server lists. Clicking that link displays a list of available public groups.

Only public groups can be used for modeling.

Static Groups

Static groups can be either public or private, and no specific permissions are required for static groups. A static group has servers that are added to and removed from the group manually. When using static groups, you first create the group, and then select the servers to populate it.

Dynamic Groups

Dynamic groups contain servers that are added to or removed from the group based on a set of user-defined rules. If the rules are changed or the servers in the environment change, servers will be added to or removed from the group automatically. Rules apply only to the group being created or modified, not to any subgroups.

Once the rules have been created, Opsware SAS will search for servers that match the criteria of that specific group, and add them to the group. When the rules are changed, Opsware SAS will search again, and the resulting group members reflect the changed criteria. Consequently, as servers are added to or removed from management using Opsware SAS, the members of the group will change automatically.

Opsware SAS calculates server group membership each time any of the following actions occur:

- After users add, delete, or change the rules for dynamic server groups.
- When attributes of servers change such that dynamic group membership could change.

Additionally, Opsware SAS automatically recalculates dynamic group membership every hour.

When a user schedules a job to run, dynamic group membership can be determined in either of the following ways:

- Based on the servers in the dynamic group when the job was scheduled.
- Based on the set of servers in the dynamic group when the job actually runs. The membership is recalculated at that time.

Public Group Modeling

With Opsware modeling, the desired state of a server is defined and then applied to servers. In the case of public server groups – static and dynamic – you can define a model consisting of applications, patches, service levels, and custom attributes, which will be applied to all servers in the group. The modeling information is attached to the group, but not to any subgroups.

If the modeling information changes, the servers in the group are not affected until the remediate operation runs on those servers. If the model has already been remediated on that server when it is removed from the group, the installed material will be removed at the next remediate process.

Manage Servers Display for Public and Private Groups

As Figure 8-3 shows, server groups appear at the top of the Manage Server list. Public Groups appear as a link at the top of the list. Private groups, if any have been created, appear next, followed by the list of individual servers.

Figure 8-3: Manage Servers Displaying Public and Private Groups – Servers and Group View

Resource Edit View Tasks Configuration Tracking							
<input type="checkbox"/>	Name ^	Host Name / IP Address	OS Version	Stage	Use	Facility	Customer
	Public Groups						
<input type="checkbox"/>	barbar , 0 Servers (Static)						
<input type="checkbox"/>	barfoo , 0 Servers (Dynamic)						
<input type="checkbox"/>	dhcp-8-071.corp.opsware.com faisal's desktop do not touch	dhcp-8-071.corp.opsware.com 192.168.8.71	Red Hat Enterprise Linux AS 3	Not Specified	Not Specified	C29	Opsware

Manage Servers List - Groups Only

When you select **View ► Groups Only** from the menu, information about the number of servers in a group, the number of groups in a group, and whether the group is static or dynamic appears in the list of groups, as Figure 8-4 shows.

Figure 8-4: Manage Servers List – Group Only View

Manage Servers (Summary View - Groups Only)

OK

Resource Edit View Tasks Configuration Tracking								
<input type="checkbox"/>	Name ^	Members		Total Servers	Type	Model Attachments	Custom Attributes	Last Use
		Servers	Subgroups					
	Public Groups	0	113	222		0	0	
<input type="checkbox"/>	A Group	0	1	0	Static	0	0	

You can modify your views of servers and server groups by selecting Summary, Hardware, Software, and Communications from the **View** menu. You can also elect to further modify your view by selecting Servers and Groups, Servers Only, or Groups Only.

Operations on Server Groups

Any operation that can be done to a server can be done to a server group, because the group acts as a container for a collection of servers, and so provides a shortcut to avoid having to repeat the same operation on each individual server.

When any of the following operations are performed on a group, they are actually performed on the servers within the group, not on the group itself.

- Run
 - Script
 - Custom Extension
 - Communication Test
- Customer
- Usage
- SAS Client operations
 - Configure Application
 - Audit Application Configurations
 - Perform Server Audit
 - Create Server Snapshot
 - Install Patch
 - Install software

Also, some operations allow users to refresh the list of servers in the group (if the user has the Allow Run Refresh Jobs permissions). Users with the correct permissions schedule a job, and before the job is run, Opsware SAS will update the members of the server groups upon which the operation is performed. The following actions allow refresh when scheduling a job:

- Run Script
- Run Custom Extension

Using Server Groups Tabs


When you view group properties, the information for the group appears in the page, as Figure 8-5 shows.

You can view group properties in either of the following ways:

- By clicking the This Group link at the top of each server group list.

- By selecting a group in the list and choosing **Resource** ► **Properties** from the menu.

Figure 8-5: Tabs Available for Server Groups

Manage Servers / Public / All Windows Servers / **Properties** 

Properties Rules Custom Attributes 0 Service Levels 0 History

The following properties describe or restrict use of the current group. Edit

Name:	All Windows Servers
Description:	
Type:	Dynamic
Status:	Active
Accessibility:	Public
Servers (at this level):	7
Groups (at this level):	0
Unique servers for all levels:	7
Date last used (by a job):	
Device Group ID:	2530039

You can use these tabs to perform the following actions for a server group.

To perform any of these actions, you must have the correct Opsware SAS permissions. See “Permissions Required for Working with Server Groups” on page 281 in this chapter for more information.

- **Properties:** This displays information about the group, such as the type of group, the number of servers in the group, and the status of the group. Clicking **Edit** allows you to change the group name and description, and to convert a dynamic group to a static group.



A created static group without servers added yet – an empty static group – can be converted to a dynamic group. Conversely, a static group that has servers cannot be converted to a dynamic group.

- **Rules:** This appears when you are viewing a dynamic group. The rules tab displays the rules used by the dynamic group to determine group membership. The rules apply to the current group only and do not apply to subgroups. Click **Edit** to change the rules for the group.

See “Creating Groups by Using Search” on page 293 in this chapter for more information about specifying rules for a dynamic group.

- **Custom Attributes:** This allows you to set custom attributes for a server group. Click **New** to add an attribute and then click **Edit** to change existing attributes. Custom attributes are not inherited by subgroups within a group hierarchy.

See “Custom Attributes for Servers” on page 336 in this chapter for more information about how custom attributes affect Opware-managed servers.

- **Service Levels:** This allows you to attach service levels to a group.
See “Service Levels” on page 340 in this chapter for more information.
- **History:** This allows you to view the changes to groups. For each action on the group (but not group members), the history displays a description, the date the action occurred, and the user who performed the action (if the group is public).

Ways to Create Server Groups

Server Groups can be created by:

- Using the New Group option from the Resource pull down menu on the Manage Servers page
- Clicking the Create Server Groups icon in the upper right corner of the Copy to Group dialog
- Performing a server search, and saving the resulting list of servers or the rules as a group

Creating Static Groups by Using the New Group Option

Static server groups require servers to be added to them manually. The servers in a static group also must be removed manually.



A created static group without servers added yet – an empty static group – can be converted to a dynamic group. Conversely, a static group that has servers cannot be converted to a dynamic group.

To create static server groups, perform the following steps:

- 1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears.
- 2 From the **Resource** menu, choose **New Group**. The New Private Static Group dialog appears, as shown in Figure 8-6.

Figure 8-6: Default New Private Static Group Dialog

Name	Type
Public Groups	Dynamic
Content Groups, Dynamic	Dynamic
Content Management Servers	Dynamic
Dynamic Content Servers	Dynamic

- 3 To create a Private Static group in the top level of Manage Servers, perform the following steps:
 1. Enter the name of the group in the Save As text box.
 2. Click **Save**.
- 4 To create a Private Static group below another group, perform the following steps:
 1. Navigate to the group below which you want to create a new group.
 2. Enter the name of the group in the Save As text box.
 3. Click **Save**.

- 5** To create a Public Static Group, perform the following steps:
 1. Click the Public Groups link in the Name and Type window, and navigate to the location in the group hierarchy where you want to create the group.
 2. Enter the name of the group in the Save As text box.
 3. Click **Save**.



The Save In drop down list is populated according to the location you drill down to in order to create your group. You can use the Save In drop down list to verify that you are in the correct location in the group hierarchy, and you can move to a different location in the hierarchy by selecting it from the Save In list.

Creating Static Groups by Using the Copy to Group Dialog

To create new server groups by copying existing server groups, perform the following actions:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears.
- 2** Navigate to the servers and groups that you want to copy and click the check boxes next to the servers and groups you want to copy.
- 3** From the **Edit** menu, choose **Copy to Group**. The Copy to Group dialog box appears.
- 4** Navigate to the place in the group hierarchy where you want to copy the servers and group then by clicking the group links displayed in the Name and Type field.
- 5** In the Options field, select either of the following options:
 - **Maintain Hierarchy**: Select this option to copy any server groups exactly as they are.
 - **Expand to a Flat List**: Select this option to copy only the servers within the group to the new group.

Each of those options displays the result of choosing that option by showing the numbers of servers and groups in the new group's hierarchy, or the number of unique servers in the flat list.



If you select the Expand to a Flat List option, and a server is a member of more than one group, that server will only appear in the list once.

6 (Optional) You can also create an entirely new group for the copied servers and groups by clicking the Create New Group icon in the upper right corner of the dialog.

A new dialog appears, prompting you to name your new group.

7 Enter the name of your newly-created group.

8 Click **OK**. The name dialog closes, and the Copy to Group dialog reappears.

9 Click **OK** on the Copy to Group dialog.

Creating Dynamic Groups by Using the New Group Option

Dynamic Server Groups are rule-based, and the servers in dynamic groups will be added or removed automatically based on the rules that you define.

The method for creating dynamic server groups is the same as for creating static server groups. The difference is that when dynamic is selected, you are presented with a page that allows you to define the rules for the group.



Dynamic groups can be converted to static groups, and all servers remain in the group, but all rules will be lost when they are converted.

To create dynamic groups using the New Groups Option, perform the following steps:

1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears.

2 From the **Resource** menu, choose **New Group**. The New Private Static Group dialog appears.

3 To create a private dynamic group, navigate to the place in the group hierarchy where you want to create the group by clicking the group links displayed in the Name and Type field.

Or

To create a public dynamic group, click the Public Groups link in the Name and Type field, and navigate to the location in the group hierarchy where you want to create the group.



The Save In drop down list is populated according to the location you drill down to in order to create your group. You can use the Save In drop-down list to verify that you are in the correct location in the group hierarchy, and you can move to a different location in the hierarchy by selecting it from the Save In list.

- 4** Enter the name of the group in the Save As text box.
- 5** In the Options field, select Dynamic.
- 6** Click **Create Rules**. The Manage Servers Properties page appears, with the Rules tab selected, as Figure 8-7 shows.

Figure 8-7: Manage Servers Properties Page with Rules Tab Selected

- 7** Select the criteria that apply to the servers you would like the group to include. See “From the navigation panel, click Servers % Search. The Search Rules page appears with the Servers tab displayed.” on page 293 in this chapter for more information.



Create as many lines of criteria as required to adequately describe your server group rules by clicking the plus button to add a new line. Conversely, to remove lines of criteria, click the minus button next to the line you want to remove.

- 8** From the Match drop down list select either “If all rules are met” or “If any rules are met.”
- 9** (Optional) Click **Search** to apply the rules to a server search to validate the results.

- 10** Click **Save** to save the rules that apply to your group.

Creating Groups by Using Search

To create groups by using search, perform the following steps:

- 1** From the navigation panel, click Servers ► Search. The Search Rules page appears with the Servers tab displayed.

To search for servers, use this tab. To search for groups, select the Groups tab.

- 2** Use the criteria to create the rules used for a server search and to identify servers for dynamic groups. The options in the user interface for specifying dynamic group rules and for using Search are the same. See “Criteria for Search and Dynamic Group Rules” on page 293 in this chapter for more information.



Create as many lines of criteria as required to adequately describe your server search or your server group rules by clicking the plus button to add a new line. Conversely, to remove lines of criteria, click minus button next to the line you want to remove.

- 3** If you are defining dynamic server group rules, click **Save** to save your rules. You can also click **Search** to use your rules to perform a server search.

Or

If you are doing a server search, click **Search** to perform the server search, or click **Save** to save the search as the rules for a dynamic group.

The New Dynamic Group dialog appears.

Criteria for Search and Dynamic Group Rules

The following table describes the rules that you can use to search for servers or to create dynamic server groups.

Note that anywhere you can enter text, you can enter a wildcard (*) character to broaden your results.

Table 8-2: Rules for Server Search and for Creating Dynamic Groups

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
PROPERTIES		

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
Agent Discovery Date: The date that the Opsware Agent was installed.	<ul style="list-style-type: none"> Is after Is before 	Drop-down lists with the day, month, and year
	<ul style="list-style-type: none"> Is within the last 	User-entered text
	<ul style="list-style-type: none"> Is today 	N/A
Agent Reporting: Whether the Opsware Agent is reporting to Opsware SAS.	<ul style="list-style-type: none"> Is Is not 	<ul style="list-style-type: none"> Has not reported OK Registration in progress Reporting error
Agent Status: Whether the Opsware Agent is reachable by Opsware SAS.	<ul style="list-style-type: none"> Is Is not 	<ul style="list-style-type: none"> Not reachable OK
Agent Version: The version of the Opsware Agent – such as 14.2.3b.	<ul style="list-style-type: none"> Contains Does not contain Is Is not 	User-entered text
Custom Attribute (any): The name of a custom attribute that is associated with the server through attachment or inheritance.	<ul style="list-style-type: none"> Contains Is 	User-entered text
Custom Attribute (local): The name of a custom attribute that is locally attached to the server,	<ul style="list-style-type: none"> Contains Is 	User-entered text
Customer: The customer or account that the server is associated with.	<ul style="list-style-type: none"> Is Is not 	Popup window of customers

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Deployment Stage: The stage the server performs within a lifecycle environment.</p>	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • In Deployment • Live • Not Specified • Offline <hr/> <p>The values that appear in this list are customizable; in addition to the values above, values specific to your environment might appear.</p> <hr/>
<p>Facility: The collection of servers managed by an Opware SAS installation.</p>	<ul style="list-style-type: none"> • Is • Is not 	<p>Popup window of facilities</p> <hr/> <p>When Opware SAS is running multimaster mode, the list can contain many facilities.</p> <hr/>
<p>Group Membership: Whether the server belongs to a group.</p>	<ul style="list-style-type: none"> • Is 	<p>Popup window of groups</p>
<p>Host name: The host name of the server – such as m004.company.com.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Name (any): This enables searching for any name or IP address associated with a server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Notes: The contents of the Notes field from the Properties tab for a server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Opsware Display Name: The user-configurable name for the server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p> <hr/> <p>By default, Opsware SAS uses the configured host name of the server until a user edits it.</p>
<p>Server Use: How the server is being used – such as Development, Staging, Production.</p>	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • Development • Not Specified • Production • Staging <hr/> <p>You can customize values that appear in this list. In addition to the values above, values specific to your environment might appear.</p>
<p>Service Level: The user-defined category that can be used as an organizational tool.</p>	<ul style="list-style-type: none"> • Is • Is attached here or below 	<p>Popup window of service levels</p> <hr/> <p>Servers can be associated with multiple service levels.</p>
<p>OPSWARE PROPERTIES</p>		

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
Application Configuration: Whether the server uses the Application Configuration feature.	<ul style="list-style-type: none"> • Is not used • Is used 	N/A
Code Deployment: Whether the server uses the Code Deployment feature.	<ul style="list-style-type: none"> • Is not used • Is used 	N/A
Configuration Tracking: Whether the Configuration Tracking feature is monitoring or backing up specific files or configurations on a server.	<ul style="list-style-type: none"> • Is off • Is on 	N/A
Lifecycle: The server states that are part of bringing a server into Opware SAS.	<ul style="list-style-type: none"> • Is • Is not 	<ul style="list-style-type: none"> • Available • Build Failed • Deactivated • Installing OS • Managed
Server ID: The internal ID Opware SAS uses to identify the server.	<ul style="list-style-type: none"> • Is • Is not 	User-entered text <hr/> In most cases, the Server ID is the same as the MID. <hr/>
SOFTWARE		
Attached Software: The software that is assigned or modeled through the Opware remediate operation – the installation process.	<ul style="list-style-type: none"> • Is • Is attached here or below 	Popup window of software

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
<p>Attached Software Policies: The software policies that is assigned or modeled through the Opsware installation process.</p>	<ul style="list-style-type: none"> • is 	<p>Popup window of software policies</p>
<p>Installed Patches: Whether a patch is installed on the server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Installed Software: The package reported installed on the server.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p> <hr/> <p>A package does not have to be installed by Opsware SAS to be reported as installed on a server.</p> <hr/>
<p>OS Version: The OS version defined by OS definitions in the OS Provisioning feature.</p>	<ul style="list-style-type: none"> • Is • Is not 	<p>Popup window of operating systems</p>
<p>Reported OS: For Windows – the version reported by the OS, for Unix – the version returned by the uname command.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>Windows Service: The names of the Windows services that are reported to Opsware SAS.</p>	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	<p>User-entered text</p>
<p>NETWORK</p>		

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
DNS Search Domains: The domains configured to be searched in the server's network settings.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
DNS Servers: The IP addresses of the DNS servers configured in the server's network settings.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
Default Gateway: The IP address of the default router.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
IP Address: Any Internet Protocol address for the server.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
MAC Address: Any Media Access Control address, which is the network interface card's unique hardware number.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
WINS Servers: The Windows Internet Naming Servers configured in the server's network settings.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
HARDWARE		

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
CPU Make and Model: The vendor name and CPU model for the server – such as GENUINEINTEL Intel(R) Pentium(R) 4 CPU 2.60GHz.	<ul style="list-style-type: none"> • Is • Is not 	Popup window of CPU makes and models
CPU Speed: The Central Processing Unit speed in gigahertz [GHz].	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text <hr/> A 600 Mhz machine should be entered as 0 . 6. <hr/>
Make and Model: The vendor name and server model for the server – such as Compaq - DL360.	<ul style="list-style-type: none"> • Is • Is not 	Popup window of server makes and models
Number of CPUs: The number of CPUs on the server.	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text
RAM: The amount of RAM on the server in megabytes [MB].	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text <hr/> To enter 1 Gigabyte, type 1024. <hr/>
Serial Number: The serial number of the server.	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text

Table 8-2: Rules for Server Search and for Creating Dynamic Groups (continued)

RULE NAME AND DESCRIPTION	OPERATORS	VALUE
Storage Make and Model: The vendor name and storage model for the server – such as WDC - WD800BB-75DKA0.	<ul style="list-style-type: none"> • Is • Is not 	Popup window of storage makes and models
CUSTOM FIELDS		
A Numeric field	<ul style="list-style-type: none"> • Does not equal • Equals • Is greater than • Is less than 	User-entered text
A String field	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
A URI field	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
A File field	<ul style="list-style-type: none"> • Contains • Does not contain • Is • Is not 	User-entered text
A Date field	<ul style="list-style-type: none"> • Is after • Is before 	Drop-down lists with the day, month, and year
	<ul style="list-style-type: none"> • Is within the last 	User-entered text
	<ul style="list-style-type: none"> • Is today 	N/A

Adding a Server to Static Groups, Both Public and Private

To add a server or a server group to a static group, perform the following steps:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears.
- 2** Navigate to the static group that you want to add servers and server groups to.
- 3** Click the check box next to the group and select **Edit ► Add Servers**. The Select Servers and Groups to Add to [group name] window opens. The window is populated with the same servers and groups visible on the Manage Servers page. You can use the Status, OS, and Customer filters to change the servers and groups that appear on the list.



When you select **Edit ► Add Servers** and then select a group, the servers in the group are added. The group itself is not added. If you want to add a group to a group, select **Edit ► Copy to Group** from the menu.

- 4** Click the check box next to the servers and groups you want to add, and click **Add** at the bottom of the window.

Adding a Server to Dynamic Groups, Both Public and Private

Servers are added to dynamic server groups automatically, based on the rules created for the group. To change the membership of a dynamic group, add, delete, or update the dynamic group rules.

To update the rules for a dynamic group, perform the following steps:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears.
- 2** Navigate to the Properties page of the dynamic group that you want to update rules for; navigate by clicking the group links in Manage Server list.
- 3** Select the Rules tab.
- 4** Click **Edit**.

- 5 To add criteria to the existing rules, click the plus (+) button next to existing criteria. The fields for the criteria appear. Enter the values for the rule. See “From the navigation panel, click Servers % Search. The Search Rules page appears with the Servers tab displayed.” on page 293 in this chapter for descriptions of these values.
- 6 To delete criteria, click the minus (-) button next to the criteria you want to delete from the rules. The criteria are removed from the page.
- 7 Click **Save**.

Groups can be added manually to a dynamic group, in either of the following two ways:

- 1 Click the check box next to the name of the server group to which you want to add a server group, and select **Edit ► Copy to Group**. Then follow the steps for creating a new group, either static or dynamic. See “Ways to Create Server Groups” on page 288 in this chapter for more information.

Or

Navigate to the server group that you want to add a server group to.

- 2 Click the check box next to “This Group” and select **Resource ► New Group**. Then follow the steps for creating a new group, either static or dynamic. See “Ways to Create Server Groups” on page 288 in this chapter for more information.

Removing Servers from Static Groups, Both Public and Private

To remove a server from a static server group, perform the following steps:



A server does not need to be deactivated to be removed from a group. You can remove a server from a Static group at any time. The Membership tab for a server displays all the server groups of which the server is a member.

- 1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears.
- 2 Navigate to the static server group that you want to remove servers from until you reach the level where the servers in question are located.



Servers can belong to more than one group, so if you want to remove a server from each group it belongs to, you must locate and remove each instance of the server from all groups.

- 3 Click the check box next to the servers you want to remove and select **Edit ► Remove from Group**.

As soon as you select that menu option, the server is removed and the screen refreshes to display the current members of the group.

Removing Servers from Dynamic Groups, Both Public and Private

Servers are removed from dynamic server groups automatically, based on the rules created for the group. To remove servers, you can create or update rules. To add rules to an existing server group, perform the following steps:

- 1 From the navigation panel, click **Servers ► Manage Servers**. The Manage Servers page appears.
- 2 Navigate to the Properties page of the dynamic group that you want to add rules to, by drilling down into the group and clicking the "This Group" link.
- 3 Select the Rules tab.
- 4 Click **Edit**.
- 5 Add one or more lines of criteria to the existing rules by following the procedure described in the "Creating Dynamic Server Groups by Using the New Group Option" topic, step 3 on page 293 or see "From the navigation panel, click Servers %0 Search. The Search Rules page appears with the Servers tab displayed." on page 293 in this chapter for more information.

Moving Servers from One Static Group to Another

The process of moving servers from one group to another is similar to copying servers from one group to another with the exception that with a move, the servers do not remain in the original group.



The **Edit ► Move** menu option is disabled when you select servers in a dynamic group. To move servers in a dynamic group, chose the **Edit ► Copy to Group** menu command.

This menu command is also disabled for public groups when you do not have permission to manage public groups.

To move servers from one group to another, perform the following steps:

- 1** From the navigation panel, click **Servers ► Manage Servers**. The Manage Servers page appears.
- 2** Navigate to the group containing the servers you want to move and select those servers.
- 3** From the **Edit** menu, choose **Move**. The Move [group name] Group dialog box appears.
- 4** Navigate to the place in the group hierarchy where you want to create the group by clicking the group links displayed in the Name and Type field.
- 5** Click **Move**.

Duplicating Server Groups

Duplicating a group is similar to copying a group. To duplicate an existing group, perform the following steps:

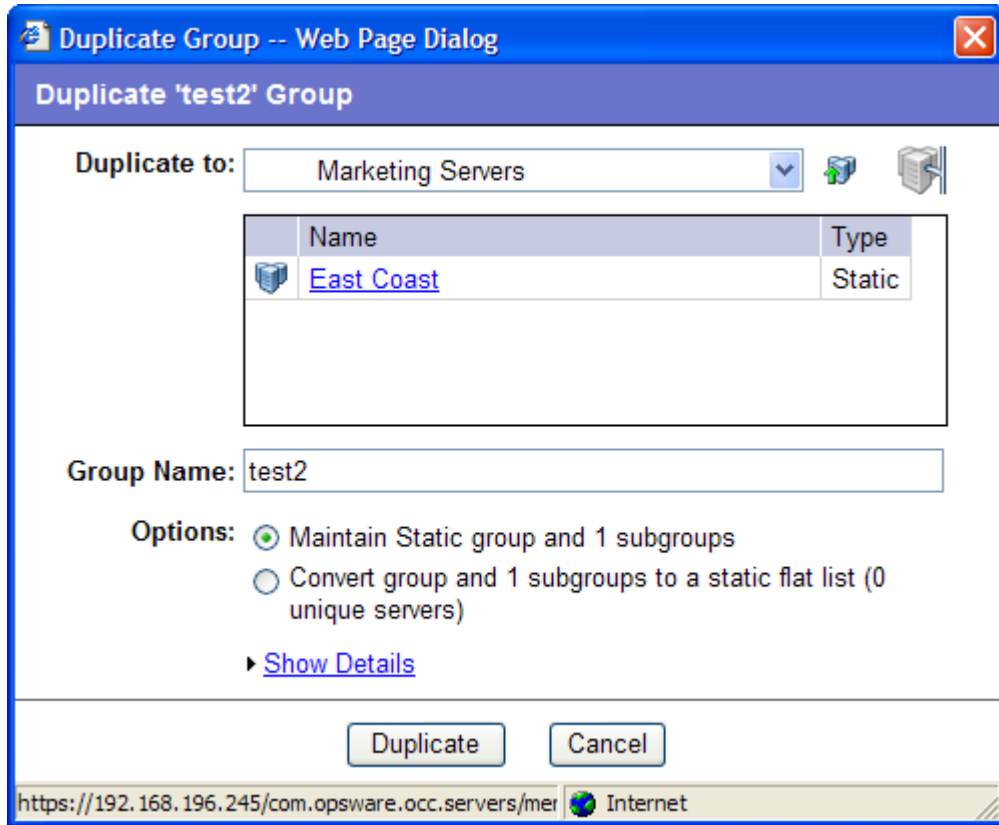
- 1** Navigate to the group that you want to duplicate.
- 2** Click the check box next to the group name.



You can only select one group at a time to duplicate.

- 3 From the **Edit** menu, choose **Duplicate Group**. The Duplicate [group name] Group dialog appears as shown in Figure 8-8.

Figure 8-8: Duplicate Group Dialog Box



- 4 Select the location for the newly-duplicated group using the Duplicate In drop down list.



The Duplicate In drop down list's default location is the location of the group you select to duplicate. Navigate through the hierarchy of groups to find the location where you want the newly-duplicated group to reside.

- 5 Enter the name of the new group.
- 6 The values on the Options field will vary depending on whether the group duplicated is static or dynamic.

- 7** If the group is static, select one of the following options:
- **Maintain Static group and <number> subgroups:** Selecting this option copies the group and its hierarchy as is.
 - **Convert group and <number> subgroups to a static flat list:** Selecting this option copies the group and flattens the hierarchy.
- 8** If the group is dynamic, select one of the following options:
- **Maintain rules & group hierarchy:** Selecting this option copies the group and leaves it as a dynamic group, it also copies any subgroups.
 - **Convert to static group, maintain hierarchy:** Selecting this option copies the group, but turns it into a static group with the current servers defined by the rules and also copies any subgroups.
 - **Convert group and <number> subgroups to a static flat list:** Selecting this option copies the group, and turns it into a static group and flattens any hierarchy.
- 9** Click **Duplicate**. The newly-duplicated group appears in the selected destination.

Rules for Deleting Server Groups

It's important to note the distinction between removing servers from a group, deleting a server, and deleting a group.

Removing servers from a group only removes the server from the selected static group, but the server itself remains in the global list of servers and is still managed by Opware SAS.

Deleting a server can only be performed on a server whose status is deactivated. Selecting the Delete Server option completely removes the server from within Opware SAS, although its history remains.

Deleting a server group removes the group, but the servers in the group still remain in the list of servers and in any other groups for which they are members.

A group cannot be deleted when any of the following conditions apply:

- Software is attached to the group or a subgroup of the group.
- Access control boundaries are attached to the groups or a subgroup of the group.
- Servers and groups are selected together for deletion.

Deleting a Server Group

To delete a server group, perform the following steps:

- 1** Click the check box next to the server group you want to delete.
- 2** From the **Edit** menu, choose **Delete Group**. A confirmation message appears, detailing the number of servers and server groups in the server group that you want to delete.
- 3** Click **OK** to complete the deletion of the server group.

The screen refreshes, showing the list of servers and groups without the deleted server group.

Server Life Cycle

This section provides information on the server life cycle within Opsware SAS and contains the following topics:

- OS Provisioning and the Server Life Cycle
- Server Properties
- Server Management Tasks Related to the Server Life Cycle
- Changing the Use and Stage Values for Servers
- Editing the Properties of a Server
- Tasks Associated with Deactivating a Server
- Deactivating a Server
- Deleting a Server from Opsware SAS
- Server Management Jobs

OS Provisioning and the Server Life Cycle

Opsware SAS is designed to enable multiple teams to work together to provision servers. The OS Provisioning feature allows IT teams to separate the tasks of readying servers for provisioning (such as mounting servers in racks and connecting them to a network) from provisioning the servers with operating systems and applications.

For example, someone mounts a new server in a rack and connects it to the Opsware build network. Next, they boot the server for the first time by using an Opsware Boot Floppy or CD or by using the network.

At a later time, a different system administrator can select the available server from the Server Pool list and provision it with an OS. In the available state, servers do not have the target OS installed and might not have access to disk resources.

During OS provisioning, servers progress through the Opsware SAS life cycle state changes:

Unprovisioned (No OS Build Agent) ➤ Available ➤ Installing OS ➤ Managed

Table 8-3 describes the Opsware SAS server life cycle values.

Table 8-3: Opsware SAS Life Cycle Values for Servers

OPSWARE LIFE CYCLE VALUE	DESCRIPTION
Server Pool Values	
Planned	<p>Indicates that a device record has been created for the server, but an Opsware build agent has not yet been installed. Servers in this stage cannot be provisioned until an OS build agent is installed.</p> <p>For more information on this unprovisioned lifecycle value, see your Opsware Administrator.</p>
Available	<p>Indicates a server on which the OS Build Agent was installed and is running, but the target OS has not been installed on the server.</p> <p>The OS Build Agent is a small agent that can run in the memory of the bare-metal server.</p> <p>See <i>Opsware® SAS User's Guide: Application Automation</i> for more information about Operating System Provisioning.</p>
Installing OS	<p>Indicates that a user is installing the target OS on the server.</p> <p>The server stays in the Server Pool list until the installation process finishes successfully. Then the server moves to the Manage Servers list.</p> <p>See <i>Opsware® SAS User's Guide: Application Automation</i> for more information about installing OS.</p>
Build Failed	<p>Indicates a server on which the OS Build Agent was installed and is running, but the installation of the target OS failed.</p> <p>The server remains in the Server Pool list with this status for 7 days before Opsware SAS deletes the entry.</p> <p>See <i>Opsware® SAS User's Guide: Application Automation</i> for more information about Operating System Provisioning.</p>

Table 8-3: Opware SAS Life Cycle Values for Servers (continued)

OPSWARE LIFE CYCLE VALUE	DESCRIPTION
Managed Server Values	
Managed	<p>Indicates a server that Opware SAS is managing. Opware SAS performs periodic reachability checks on managed servers.</p> <p>After a server reaches this life cycle state, the entry for the server moves from the Server Pool list to the Manage Servers list. On managed servers, you can use Opware SAS to install applications and patches.</p>
Deactivated	<p>Indicates an Opware-managed server that was removed from service. However, the server's history still exists in Opware SAS. Deactivated servers are not reachable.</p>

Table 8-4 describes server states in Opware SAS in regard to the server life cycle.

Table 8-4: Server Status Icons in Opware SAS


SERVER ICON	DESCRIPTION
	<p>Planned</p> <p>Indicates that a device record has been created for the server, but an Opware OS Build Agent has not yet been installed on it. Servers in this stage cannot be provisioned until the OS Build Agent is installed.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>

Table 8-4: Server Status Icons in Opware SAS





SERVER ICON	DESCRIPTION
	<p>Unprovisioned – Unreachable</p> <p>Indicates a server that has been registered with the core via the Opware OS Build Agent, but has not reported as ready for provisioning recently. This may be due to networking problems between the server and the Opware core or the server having been disconnected or powered off.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Unprovisioned – Reachable</p> <p>Indicates a server that has been registered with the core via the Opware OS Build Agent and is available to have a target OS installed on it.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Provisioning – Unreachable</p> <p>Indicates a server on which the OS Provisioning feature was in the process of installing the target OS, but for some reason stopped because the server is unable to communicate with the Opware core.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Provisioning – Reachable</p> <p>Indicates a server on which the OS Provisioning feature is in the process of installing the target OS.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>

Table 8-4: Server Status Icons in Opsware SAS




SERVER ICON	DESCRIPTION
	<p>Provisioning Failed – Unreachable</p> <p>Indicates an available server on which an error occurred while the OS Provisioning Subsystem was installing a target OS, and that the server is not able to communicate with the Opsware core.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Provisioning Failed – Reachable</p> <p>Indicates an available server on which an error occurred while the OS Provisioning Subsystem was installing a target OS.</p> <p>In the SAS Client, appears in the Unprovisioned Server list.</p> <p>In the SAS Web Client, appears in the My Jobs panel home page, in the My Jobs page, and in the Server Pool list.</p>
	<p>Managed – Reachable</p> <p>Indicates a server has an An Opsware Agent is running on it and that it is able to communicate with the Opsware core.</p> <p>In the SAS Client, appears in the All Managed Servers list and Virtual Servers list.</p> <p>In the SAS Web Client, appears in the My Jobs panel in the home page, in the list in the My Jobs page, in the Manage Servers list, and in the server lists in the Opsware wizards.</p>

Table 8-4: Server Status Icons in Opware SAS




SERVER ICON	DESCRIPTION
	<p>Managed – Unreachable</p> <p>Indicates a managed server cannot communicate with the Opware core (it is Not Reachable).</p> <p>If you want to discover reasons why the managed server is unreachable, you can run a Communication Test. See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for more information.</p> <p>In the SAS Client, appears in the All Managed Servers list and Virtual Servers list.</p> <p>In the SAS Web Client, appears in the My Jobs panel in the home page, in the list in the My Jobs page, in the Manage Servers list, and in the server lists in the Opware wizards.</p>
	<p>Unmanaged</p> <p>Indicates the server is unmanaged, which means it does not have an Opware agent installed on it.</p> <p>For unmanaged virtual servers, this means that someone created a VMware Virtual Machine (VM) or Solaris local zone outside of Opware SAS and thus does not have an Opware Agent installed on it.</p> <p>For virtual servers, this state could also mean that the VMware VM is has not yet been provisioned, or that your user belongs to a group that does not have permissions to perform operations on this virtual server.</p> <p>For more information on installing an Opware agent on an unmanaged server, see Chapter 4, “Opware Agent Management” on page 99 of this guide.</p>
	<p>Deactivated</p> <p>Indicates a server that was deactivated in Opware SAS so that it is currently not managed and is no longer reachable.</p> <p>Appears in the Manage Servers list and in the server lists in the Opware wizards (however, it is not selectable in the wizards).</p>

Table 8-4: Server Status Icons in Opsware SAS









SERVER ICON	DESCRIPTION
	<p>Scheduled</p> <p>Indicates a server that is scheduled for an operation (install software, uninstall software, and so forth).</p> <p>In the SAS Client, appears in the Job Logs list.</p> <p>In the SAS Web Client, appears in the My Jobs panel in the home page and in the list in the My Jobs page.</p>
	<p>Error</p> <p>Indicates a managed server on which an error occurred while Opsware SAS was installing or uninstalling software.</p> <p>Appears in the My Jobs panel in the home page and in the list in the My Jobs page.</p>
	<p>Warning</p> <p>Indicates a managed server on which a warning occurred while Opsware SAS was installing or uninstalling software.</p> <p>Appears in the My Jobs panel in the home page and in the list in the My Jobs page.</p>
	<p>Application Configuration Out of Sync</p> <p>Indicates a managed server on which the configuration file on the server is out of sync with the Application Configuration Template (Opsware model).</p> <p>Appears only in the Application Configuration feature and the server list in the SAS Client.</p>
	<p>Static Device Group</p> <p>Indicates a static server group. The same states that apply to single servers apply to groups.</p> <p>See “Server Groups” on page 280 in this chapter for information about the different types of server groups.</p>

Table 8-4: Server Status Icons in Opware SAS

SERVER ICON	DESCRIPTION
	Dynamic Device Group Indicates a dynamic server group. The same states that apply to single servers apply to groups.
	Public Static Device Group Indicates a public and static server group. The same states that apply to single servers apply to groups.
	Public Edenic Device Group Indicates a public and dynamic server group. The same states that apply to single servers apply to groups.

Server Properties

Figure 8-9 shows the Server Properties columns. Table 8-5, Table 8-6, and Table 8-7 describe the Status, Stage, and Use properties for managed servers.


Figure 8-9: Server Properties Columns in the Manage Servers List

Manage Servers (Summary View) ?




All Statuses ▼ | All Operating Systems ▼ | All Stages ▼ | All Uses ▼

All Customers ▼ | All Manufacturers ▼ | All Models ▼

Managed & Deactivated ▼

Update 

Resource Edit View Tasks Configuration Tracking

<input type="checkbox"/>	Name ▲	Host Name / IP Address	OS Version	Stage	Use	Customer
 Public Groups						
<input type="checkbox"/>	 core.tr3.opsware.com	core.tr3.opsware.com 172.16.36.18	Red Hat Enterprise Linux AS 3	Not Specified	Not Specified	Opware
<input type="checkbox"/>	 mh01.tr3.opsware.com	mh03 172.16.36.34	Windows 2000	Not Specified	Not Specified	Not Assigned



The Status property is represented by an icon in the first column in the Manage Servers list.

Status (short for Agent Status) is set automatically by Opware SAS.

Opware SAS toggles each server between OK and Not Reachable by reachability checks.

The Status value specifies the ability of Opware SAS to manage servers. Opware SAS automatically detects the status of servers. To verify the current status of a server, click Update in the Server Properties page for that server.

Table 8-5: Values for the Status Property for Managed Servers

STATUS VALUE	DESCRIPTION
OK	<p>Server is manageable by Opware SAS. Represented as text (OK) in the properties page for a server. Represented as an icon in the Manage Servers and Server Pool lists:</p> 
Not Reachable	<p>Server is unreachable by Opware SAS due to an error (for example, it cannot connect to the Opware core); automatically set by Opware SAS. Represented as text (Not Reachable) in the properties page for a server. Represented as an icon in the Manage Servers list:</p>  <p>If you want to discover reasons why the managed server is unreachable, you can run a Communication Test. See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for more information.</p>

Stage (short for Deployment Stage) is set by a user.

The Stage value specifies the stages of deployment for servers; for example, a server is live or offline.

Your Opware administrator can change the values for the Stage property. By default, Opware SAS is installed with the following Stage values.

Table 8-6: Values for the Stage Property for Managed Servers

STAGE VALUE	DESCRIPTION
In Deployment	Initial stage after being fully initialized.

Table 8-6: Values for the Stage Property for Managed Servers

STAGE VALUE	DESCRIPTION
Live	Your organization defines the meaning of this stage.
Not Specified	The default value for a server. Cannot be changed by the Opware administrator.
Offline	Your organization defines the meaning of this stage.
Ops Ready	Your organization defines the meaning of this stage.

Use (short for Server Use) is set by a user.

The Use value specifies how an organization is utilizing servers. For example, a server is a staging server. Users set this property for servers.

By default, Opware SAS is installed with the following Use values. Except for the Staging, Production, and Not Specified values, an Opware administrator can change the default values. The CDR feature depends on the Staging and Production values. Therefore, these default values cannot be changed or deleted.

Table 8-7: Values for the Use Property for Managed Servers

USE VALUE	DESCRIPTION
Development	A server that is not being used in production.
Not Specified	The default value.
Production	Fully live in-use servers (includes Opware core servers).
Staging	A staging server for production.

Server Management Tasks Related to the Server Life Cycle

Managing servers in Opware SAS involves the following standard tasks:

- Bringing a new server into Opware SAS so that it appears in the Server Pool
See *Opware® SAS User's Guide: Application Automation* for more information about OS Provisioning.
- Installing an operating system on a server
See *Opware® SAS User's Guide: Application Automation* for more information about OS Provisioning.

- Installing a patch

See *Opware® SAS User's Guide: Application Automation* for more information on installing patches.

- Installing a software

See *Opware® SAS User's Guide: Application Automation* for more information on installing software.

- Re provisioning a server with a new OS

See *Opware® SAS User's Guide: Application Automation* for more information about OS Provisioning.

You can re provision Solaris and Linux servers so that they are running another version of the same OS so long as the hardware supports that new version of the OS.

You can re provision servers built by Opware SAS and Opware-managed servers by using this feature.



You cannot re provision a Linux server so that it runs a Windows OS.

- Deactivating a managed server so that Opware SAS no longer manages it.

See “Tasks Associated with Deactivating a Server” on page 322 in this chapter for more information.

You accomplish server management tasks by using the following menus in the Manage Servers list:

- Resource: Allows to create new server groups, view properties of servers.
- Edit: Allows you to add servers to a group, delete server groups, remove servers from a group, deactivate servers.
- View: Allows you to view the summary, hardware, and software information of servers and server groups.
- Tasks: Allows you perform tasks such as running scripts, custom extensions and running communication tests.
- Configuration Tracking: Allows you to edit, and reconcile tracking policies.

Changing the Use and Stage Values for Servers

Perform the following steps to change the Use and Stage values for multiple servers simultaneously:

- 1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server that you want to deactivate.

Or

Search for the server that you want to deactivate.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

- 2 Select the servers that you want different Use or Stage values for.
- 3 Choose **Edit ► Usage** from the menu above the Manage Servers list. A window prompts you to select different values, as Figure 8-10 shows.

Figure 8-10: Edit Server Popup Window

Server	Facility	Stage	Use
172.16.36.18 - core.tr3.opware.com	DATACENTER1	current: Not Specified Not Specified ▼	current: Not Specified Not Specified ▼

Save Changes Cancel

- 4 Select the Use and Stage values from the lists.
- 5 Click **Save Changes**. The window closes and the Manage Servers list refreshes with the updated values.

Editing the Properties of a Server



You can edit a server only if you have permission in the SAS Web Client to access the customer to whom the server is associated.

When you edit the properties of a server, the server itself does not change; how Opware SAS views it changes. Perform the following steps to edit the properties of a server:

- 1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server whose properties you want to edit.

Or

Search for the server that you want to edit.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

- 2** Click the Server Display name. The Properties page for the server appears.
- 3** Change any of the following properties for the server:
 - To change the name that appears in the SAS Web Client, edit the text in the Name field.
 - To change the description of the server, edit the Notes field.
 - To change the customer associated with the server, select a different customer from the list. Your Opware administrator defines the options for customer selections. Contact your Opware administrator if the list does not contain the customer that you want to associate with this server.



You cannot change the customer associated with a server when the server is part of a CDR service, synchronization, or sequence. See the *Opware[®] SAS Policy Setter's Guide* for more information.

- To change the Use or Stage of the server, make your changes in either of those lists.
See “Server Properties” on page 316 in this chapter for more information.
- To change whether configuration tracking is enabled or disabled for the server, select a value from the list.
See “Configuration Tracking” on page 463 in Chapter 13 for more information.

- 4** To save your changes, click **Save**.



To change the custom attributes of the server, select the Custom Attributes tab. The Manage Servers: Custom Attributes page appears. See “Managing Custom Attributes” on page 337 in this chapter for more information.

Tasks Associated with Deactivating a Server

You will want to deactivate a server when Opware SAS removes the server from management. For example, you are moving the server to a warehouse for storage. Additionally, you might choose to deactivate a server when you need to rebuild it from scratch, without using the OS Provisioning feature.

When you deactivate a server, information about the server remains in the Opware Model Repository for auditing purposes.

After you deactivate a server, you can reactivate it by re-installing an Opware Agent with the Opware Agent Installer and the `--clean` command line option.

See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for more information.

When you deactivate a server, you accomplish the following tasks:

- Remove custom attributes from the server.
- Delete any configuration tracking policies from the server that are associated with backups.
- Set the server life cycle value to Deactivated.



You cannot deactivate a server when it is part of a CDR service, synchronization, or sequence. See the *Opware® SAS Policy Setter's Guide* for more information.

Deactivating a Server

Perform the following steps to deactivate a server:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server that you want to deactivate.

Or

Search for the server that you want to deactivate.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

- 2** Select the servers that you want to deactivate.

- 3 Choose **Edit ► Deactivate Server** from the menu above the Manage Servers list. A confirmation dialog box prompts you to confirm the deactivation.
- 4 Click **OK**. The Manage Servers list refreshes and the server appears with a deactivated icon.

Deleting a Server from Opsware SAS

When you want to remove all record of a server from Opsware SAS, you can delete it.



You must deactivate a server before you can delete it from Opsware SAS.

When you delete a server from Opsware SAS, it has these effects:

- Deletes all job information in the My Jobs feature
- Deletes the server from the Model Repository

Perform the following steps to delete a server:

- 1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server that you want to delete.
Or
Search for the server that you want to delete.
See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.
- 2 Select the servers that you want to delete.
- 3 Choose **Edit ► Delete Server** from the menu above the Manage Servers list. A confirmation dialog box prompts you to confirm the deletion.
- 4 Click **OK**. The Manage Servers list refreshes and the server disappears from the list.

Server Management Jobs

This section provides information about server management jobs within Opsware SAS and contains the following topics:

- My Jobs

- My Jobs Display Information
- My Jobs in the Opware SAS Web Client
- Jobs in SAS Client
- Viewing Job Details in the Opware SAS Web Client
- Viewing My Job Details from inside the SAS Client

My Jobs

The My Jobs information is available only on a per-user basis. You cannot log in as an Opware administrator to see the jobs that other Opware users have run. The My Jobs information appears in two places in the SAS Web Client:

- A panel on the SAS Web Client home page that lists your most recent six jobs
- A page (accessed by clicking My Jobs in the navigation panel) that lists all the jobs that you have run

Opware SAS maintains information about the server operations that you have run for the last 30 days in the My Jobs list. By default, the jobs are deleted from the Opware Model Repository after 30 days. (The bottom of the My Jobs page indicates how long this interval is set for the Opware SAS installation at your organization.)

My Jobs Display Information

For each job, the My Jobs lists display the following information:

- The name of the job, which is a link to a page that displays more detailed information about the job
- The date and time the job started or is scheduled to start (using your preference for time display)
- The number of servers that the job affects
- The status of the job:
 - Scheduled
 - In Progress
 - Completed
 - Completed with errors
 - Completed with warnings

- You can search for an existing Job by the Job's ID. On the Home page, select Job from the drop-down list and enter a Job ID and click **Go**.

My Jobs in the Opsware SAS Web Client

The My Jobs feature in the Opsware SAS Web Client provides information about the following Command Engine scripts:

- OS provisioning
- CDR requests
- Distributed script execution
- Custom Extensions

Jobs in SAS Client

Jobs feature in the SAS Client displays job logs about the following SAS Client jobs:

- Creating snapshots
- Pushing or Auditing an Application Configuration
- Auditing Servers
- Creating Server Snapshots
- Remediating policies
- Running OS Sequence
- Any jobs scheduled to be run at a future date

Jobs in the SAS Client appears in the Jobs Logs feature window.

Viewing Job Details in the Opware SAS Web Client

Perform the following steps to view the job details:

- 1 From the SAS Web Client home page, click the link in the My Jobs panel for the job that you want to view, as Figure 8-11 shows.














Figure 8-11: My Jobs Panel in the SAS Web Client Home Page

My Jobs					See All (22)
Name	Start Time	Servers	Groups	Status	
 Run Custom Extension	(not set)	4	0	Cancelled	
 Run Script	Wed Oct 31 21:45:00 2007	4	0	Scheduled	
 Run Script	Tue May 31 21:22:06 2005	3	0	Completed with errors	
 Audit Servers [Launch OCC Client]	Tue May 31 21:00:48 2005	2	0	Completed	
 Create Snapshot [Launch OCC Client]	Tue May 31 20:57:05 2005	1	0	Completed	
 Audit Servers [Launch OCC Client]	Tue May 31 20:50:09 2005	2	0	Completed with warnings	

Or

From the navigation panel, click My Jobs and then click the link for the job to open a window that shows the details of the job, as Figure 8-12 shows.

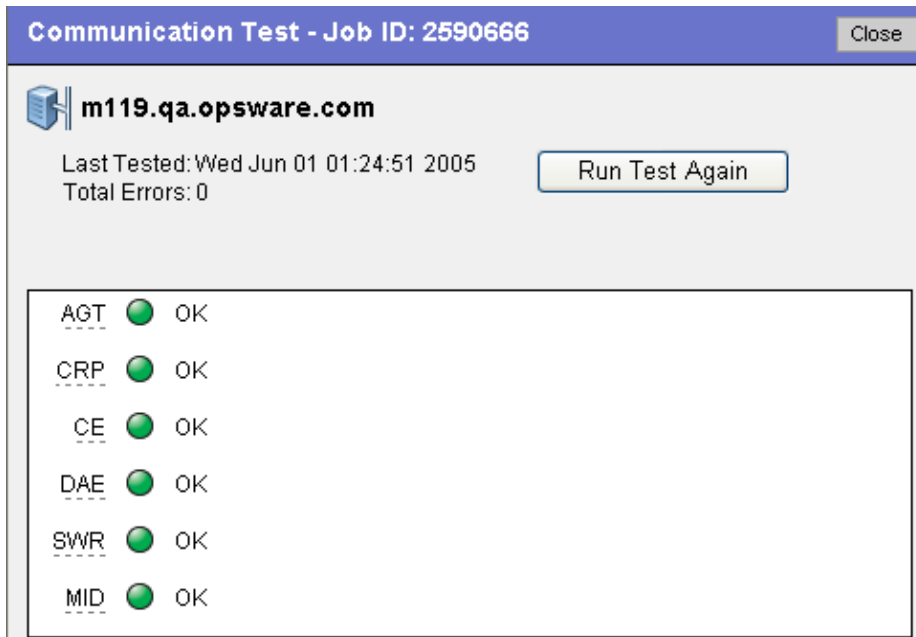
Figure 8-12: My Jobs Page Accessed from the Navigation Panel

30 Total						
Job ID	Job Type	Start Time	Servers	Groups	Status	
 1440666	Run Custom Extension	(not set)	4	0	Cancelled	
 1450666	Run Script	Wed Oct 31 21:45:00 2007	4	0	Scheduled	
 1700666	Audit Servers [Launch OCC Client]	Tue May 31 22:29:54 2005	2	0	Completed with errors	
 560667	Audit Servers [Launch OCC Client]	Tue May 31 22:19:18 2005	2	0	Completed with errors	
 550667	Audit Servers [Launch OCC Client]	Tue May 31 22:16:50 2005	2	0	Completed with errors	
 1630666	Audit Servers [Launch OCC Client]	Tue May 31 22:12:26 2005	2	0	Completed with errors	
 1580666	Audit Servers [Launch OCC Client]	Tue May 31 22:04:27 2005	2	0	Completed with errors	
 1570666	Audit Servers [Launch OCC Client]	Tue May 31 22:00:17 2005	2	0	Completed with errors	
 1560666	Audit Servers [Launch OCC Client]	Tue May 31 21:58:35 2005	2	0	Completed with errors	
 1550666	Audit Servers [Launch OCC Client]	Tue May 31 21:57:33 2005	2	0	Completed with errors	
 1460666	Run Script	Tue May 31 21:22:06 2005	3	0	Completed with errors	
 1240666	Audit Servers [Launch OCC Client]	Tue May 31 21:00:48 2005	2	0	Completed	
 1230666	Create Snapshot [Launch OCC Client]	Tue May 31 20:57:05 2005	1	0	Completed	

The My Jobs page displays the operations that you performed.

Click **View Details** to see detailed information about the job. The My Jobs information contains a build log for the job. This build log contains any error messages that Opware SAS generates. See Figure 8-13.

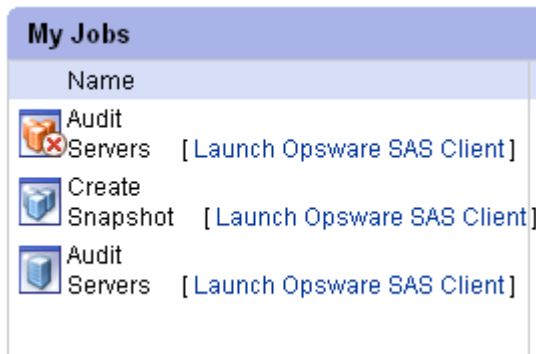
Figure 8-13: Communication Test Details Page in the My Job Window



Viewing My Job Details from inside the SAS Client

You can also view job details from inside the SAS Client. If the job was run from inside the SAS Client, you will see a link next to the job named Launch SAS Client, as shown in Figure 8-14.

Figure 8-14: My Jobs with link to SAS Client



To launch the SAS Client and view the job details, click the link.

Server Management Scheduling and Notification

This section contains the following topics:

- Scheduling a Job
- Sending Email Notification

The time used for the scheduled job is specified in the user's preferred time zone (which can be modified in My Profile). If the user does not have a preferred time zone set, the time zone is derived from the Opware SAS core server (usually UTC).

Scheduling a Job

Perform the following steps to schedule server management tasks:

- 1** In the Schedule and Notify page of an Opware Wizard, choose the Run Now option to execute the operation immediately or choose the Specify Time Option to schedule the operation at a later date and time. See Figure 8-15



The time used for the scheduled job is specified in your preferred time zone which can be modified in My Profile. If you do not have the preferred time zone set, the time zone is derived from the Opware SAS core server (usually UTC).

- 2** When you schedule a job for a server group, you can specify how the members of the group are determined. The membership of a dynamic server group changes based on the changes in your operational environment. If you have "Allow Run Refresh Jobs" permissions, you will see additional options. Select either of the following options:
 - **Option 1:** Membership is determined based on the "Time of Confirm Selection." Select this option to run the job on the servers that were in the group when you scheduled the job. Changes to the group membership do not affect the list of the servers that the job will run on.

- **Option 2:** Membership is updated when the job runs. Select this option to recalculate the group membership prior to running the job. Changes to group membership are reflected in the list of servers that the job will run on.

Figure 8-15: Scheduling a Job in an Opsware Wizard

Run Custom Extension

Schedule and Notify

Select the time and date for this job to run. You can choose to be notified after the job runs.

Schedule: Run Now Specify Time

March 07 2005 23 45

Notify: None Condition Recipients

on any result ssunderrajan@opsware.com,

Options: Run the job on the servers from the Groups based on the time of Confirm Selections. At the scheduled time, update the list of servers from the groups (0) selected prior to running the job.

Cancel < Previous Run >

- 3 Additionally, you can view a scheduled job in the My Jobs page and change the date and time for the job to run, or cancel the job entirely. (Click the name of a scheduled job to open a window to change the date or time that the job will run or cancel it.)

Sending Email Notification

The email notification feature provides you with an option to receive an email summarizing the job details when a job is over, and to notify others at the address they have registered with Opsware SAS.

You have the option of sending the notification

- On the job success only
- On the job failure only
- On any result

You can also send notification to various people based on the condition of the job. For example, you can select to send the notification to your manager only on the job success, select to send the notification to yourself on any result of the job, and select to send the notification to support only on the job failure.

To send an email about the job details, choose the Condition option on the Schedule and Notify page and set the parameters to send an email when the operation is completed. You can choose to have an email sent on any result, if the operation fails, or if the operation is successful. To add another email recipient, click the plus (+) button next to the Recipients field. See Figure 8-16.

Figure 8-16: Notifying about a Job in the SAS Web Client

Install Template - Microsoft Internet Explorer

Install Template

- Select Template
- Select Servers
- Confirm Selections
- Preview
- Schedule and Notify**
- Install

Schedule and Notify

Select the time and date for this job to run. You can choose to be notified after the job runs.

Schedule: Run Now
 Specify Time
September 22, 2004 11:30

Notify: None
 Condition
on any result Recipients: ssunderrajan@opsware.com

Cancel < Previous Install >

Time-Outs for Server Management Jobs

Table 8-8 describes the time-out values that apply to the server management operations in Opware SAS.

Table 8-8: Time-Outs in Opware SAS

TIME OUT (MINUTES)	OPSWARE SAS OPERATION
420 (7 hours)	Reconciling software (installation and uninstallation).
2	Starting Command Engine sessions in response to a command. If the Opware Agent does not start executing the command within this time, the command will time out and the Command Engine script will continue.
30	<p>Responding to a command (for example, after a reboot, the maximum time to wait until a server responds) or sending a message to the Command Engine from the Opware Agent.</p> <p>If the Opware Agent does not respond to the Command Engine at least once during this interval, the command will time out and the Command Engine script will continue.</p> <p>Opware SAS polls the Opware Agent every 15 minutes and if the Opware Agent fails to respond two consecutive times, the command will time out.</p>

Customizing the Monitor Time-Out Duration

If you would like to set a different monitor time-out duration, you can create a custom attribute named `OPSW_reconcile_monitor_timeout` and change the number of minutes before a time out occurs. For each type of hardware running in your operational environment, you can set a custom attribute with the time-out duration that you want. To set a time-out duration for a type of hardware, click **Environment** ► **Hardware** in the navigation panel. Then, navigate to the type of hardware that you want to add a custom attribute for.

During remediate, a periodic heartbeat occurs between the Opware Agent and the Command Engine to ensure that the agent is still responsive. This setting controls the maximum amount of time that can pass between these heartbeat messages. Typically,

you only need to increase this setting if you install software that reboots the server, and the time that it takes for the server to reboot and for the agent to restart exceeds the default value.

Custom Fields for Servers

This section provides information on custom fields for servers within Opsware SAS and discusses the following topics:

- Overview of Custom Fields for Servers
- Changing the Value for a Custom Field

Overview of Custom Fields for Servers

In Opsware SAS, you can store custom server data that is specific to your operational environment. These fields were created specifically for your Opsware SAS installation – all servers in an Opsware SAS installation contain the same number and type of custom fields. Custom fields can contain files, URLs, text strings, numbers, and dates.

In addition to adding files, URLs, text strings, numbers, and dates, you can use custom fields to search for servers based on a value stored in a custom field. You can also use a custom field as criteria to create a dynamic server group.



In order for the custom fields to appear in the Manage Server: Properties page, you will have to initially create a custom field. To create a custom field, you will need to install the `custFields.py` Custom Extension which is available only from the Content Starter Pack. Contact your Opsware Technical Support for assistance in installing the `custFields.py` Custom Extension in Opsware SAS.

Typed Data Supported for Custom Fields

The custom fields designated for your operational environment will vary. However, the custom fields created for your environment support values with the following data types:

- **Number:** The value provided must be a long integer.
- **Short String:** A text string that must be less than or equal to 4000 characters.
- **Long String:** A text string with no length restrictions. Custom fields with this type cannot be used in search or in the rules for dynamic server groups.

- **Date:** The value will be verified for correctness.
- **File:** Indicates a file attachment.
- **URI:** A Uniform Resource Identifier string, which is validated as a URI.

Opware SAS validates the value you enter in a custom field based on the data type specified for the field.

Uses of Custom Fields

The custom fields designated for your operational environment will vary. However, you can use custom fields to accomplish any of the following goals:

- To store the date of patch installation
- To assign a severity rating between 1 and 10 to a Hotfix
- To store an ID from an internal bug tracking system with its associated patch
- To store a JPEG image of the back of a server and have that JPEG associated with that server
- To store a Microsoft Word document describing the disaster recovery steps for a server or group of servers
- To search for a server based on the value of a custom field

Changing the Value for a Custom Field

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server whose custom fields you want to change.

Or

Search for the server whose custom fields you want to change.

- 2 Click the server name. The Manage Servers: Properties page appears. Scroll to the Custom Fields section of the page. The custom fields that appear in the properties page are specific to your operational environment. Figure 8-17 shows an example of the types of custom fields that can appear for a server.

Figure 8-17: Custom Fields That Appear for a Server

CUSTOM FIELDS	
Date to be installed	04 October 2004 [Calendar Icon] 0 00 TVT Unset
External OSS system ID	CQ12345 ... Enter up to 4000 characters in this field
Microsoft bulletin	http://www.microsoft.com/bulletin/hotfixes/Q23909.html [Edit] Unset
Severity	4 Please enter an integer with a maximum of 18 digits
Support document	support.doc This is the support document for this patch. Remove
Save Cancel	

- 3 To change a value in a field requires a number or text, enter the value in the field.
- 4 To add a file, click **Browse** and select the file from the dialog box.
- 5 To remove a file, click **Remove**.
- 6 To specify a URL, enter the URL in the field or click **Edit** to change an existing URL.
- 7 To add or change a date, click the [Calendar Icon] icon and select the date or enter the date in the field by selecting the appropriate day, month, and year from the drop-down lists.
- 8 Click **Save**.

Custom Attributes for Servers

This section provides information on custom attributes for servers within Opware SAS and contains the following topics:

- Overview of Custom Attributes for Servers
- Managing Custom Attributes
- Adding Server Custom Attributes
- Editing Server Custom Attributes
- Deleting Server Custom Attributes

Overview of Custom Attributes for Servers

Users often need to store specific miscellaneous information in the Opsware Model Repository to facilitate server or application installation and configuration, scripting, or other purposes.

The SAS Web Client provides a data management function by allowing users to set custom attributes for servers. These custom attributes include setting miscellaneous parameters and named data values. Users can write scripts that use these parameters and values when performing a variety of functions, including network and server configuration, notifications, and CRON script configuration.

Custom attributes can be accessed by software packages at installation time to configure settings that might be unique to the installation.

For information about how to set custom attributes required by the software running on a specific server, contact the group responsible for packaging your applications, as Figure 8-18 shows.

Figure 8-18: Custom Attributes Set for a Server

[Return to Manage Servers](#)

Properties	Network	Membership	Attached Nodes	Installed Packages	Custom Attributes	Config Tracking	History
<input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Revert"/>							
Name ▾		Value				Source	
OPSW.reprovision_device_attributes_to_preserve		kernel_arguments reboot_c...				Operating Systems / Red Hat Enterprise Linux AS 3 / Not Assigned (Operating Systems)	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>							

Managing Custom Attributes



Do not edit or remove custom attributes without verifying that the change you are making does not impact other users or critical Opsware operations.

To set custom attributes that affect a specific server, use the Manage Servers list. After locating the server and displaying the server properties, select the Custom Attributes tab. The SAS Web Client displays the currently defined custom attributes for the selected server.

When you add or edit server custom attributes using the SAS Web Client, Opsware SAS removes leading and trailing whitespace characters from custom attribute values.

See "Adding Server Custom Attributes" on page 338 in this chapter for more information.

You can also set custom attributes to a software policy. See the *Opsware® SAS Policy Setter's Guide* for more information.

Additionally, you can set custom attributes that affect every server associated with a specific customer or for every server in a facility. Navigate to the customer or facility where you want to set attributes. Select Environment ► Customers or Facilities in the navigation panel, and click the correct name in the list. Select the Custom Attributes tab, and add attributes for all the servers associated with the customer or located in the facility. When you use this option, you define custom attributes at a customer-specific or facility-specific level. The procedure to add custom attributes to a customer or facility is the same as adding custom attributes to individual servers.

Additionally, you can add custom attributes for a server group by viewing a server group, and then selecting the Custom Attributes tab for that group. The procedure to add custom attributes to a server group is the same as adding custom attributes to individual servers.

Adding Server Custom Attributes

For information about how to set custom attributes required by the software running on a specific server, contact the group responsible for packaging your applications.

Perform the following steps to add a custom attribute for a server:

1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server for which you want to add custom attributes.

Or

Search for the server for which you want to add custom attributes.

2 Click the display name of the server. The Manage Servers: Server Properties page appears.

3 Select the Custom Attributes tab. The Manage Servers: Custom Attributes page appears.

4 Click **New**.

5 Enter the name and value for the custom attribute that you want to add.

6 Click **Save**.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information

Editing Server Custom Attributes



If you want to change the name of a custom attribute entry, you need to create a new custom attribute and delete the old custom attribute.

Perform the following steps to edit custom attributes for a server:

- 1 From the navigation panel, click Servers ► Manage Servers or Server Pool. The Manage Servers page appears. Browse the list to find the server for which you want to edit custom attributes.

Or

Search for the server for which you want to edit custom attributes.

- 2 Click the display name of the server. The Manage Servers: Server Properties page appears.
- 3 Select the Custom Attributes tab to change the custom attributes of the server. The Manage Servers: Custom Attributes page appears.
- 4 Click the attribute name link for the custom attribute that you want to change.
- 5 Update the value of the custom attribute.
- 6 Click **Save** to save your changes. The Manage Servers: Custom Attributes page reappears with the updated value.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

Deleting Server Custom Attributes

Perform the following steps to delete custom attributes for a server:

- 1 From the navigation panel, click Servers ► Manage Servers or Server Pool. The Manage Servers page appears. Browse the list to find the server from which you want to remove custom attributes.

Or

Search for the server from which you want to remove custom attributes.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

- 2** Click the display name of the server. The Manage Servers: Server Properties page appears.
- 3** Select the Custom Attributes tab. The Manage Servers: Custom Attributes page appears.
- 4** Select the check box for the custom attribute that you want to delete.
- 5** Click **Delete**. The SAS Web Client displays a confirmation page.
- 6** Click **OK** to delete the custom attribute.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

Service Levels

This section provides information about service levels within Opware SAS and contains the following topics:

- Overview of Service Levels
- Adding a Service Level to the SAS Web Client
- Editing a Service Level
- Ways to View the Service Level for Servers
- Assigning a Server to a Service Level
- Removing a Server from a Service Level

Overview of Service Levels

Service levels are user-defined categories that enable you to group servers in an arbitrary way and design your own organizational schemes. For example, you can organize your servers by functionality (finance, engineering, and so forth) or tier (Web, application, and database) or by ontology (development, staging, and production).

You can also create service levels to indicate the Service Level Agreement (SLA) for the servers that your IT organization manages. For example, you might create service levels to denote Silver, Gold, and Platinum services.

Please note that assigning servers to service levels does not cause Opware SAS to operate any differently with respect to those servers. When you first use service levels, the categories will be fairly empty and by default, when an Opware Agent is installed on a server in the operational environment, the server will be added to the UNKNOWN Service Level.

Adding a Service Level to the SAS Web Client

Perform the following steps to add a service level to the SAS Web Client:

- 1** From the navigation panel, click Environment ► Service Levels. The Service Levels page appears.
- 2** Navigate the hierarchy of service levels until you reach the point in the hierarchy where you want to add a new service level, as Figure 8-19 shows.

Figure 8-19: Service Level Hierarchy

The screenshot shows the 'Service Levels > OTHER' page. At the top, there is a breadcrumb 'Service Levels > OTHER' and a help icon. Below this, there is a green cube icon representing the 'OTHER' service level, with a 'Details' button and an 'Add' button. Underneath the icon, it says 'No Sub-Nodes'. Below this is a table with tabs for 'Properties', 'Custom Attributes 0', 'Members 0', 'Config Tracking', 'Templates 0', and 'History'. The 'Properties' tab is active, showing a message: 'Cannot edit or delete this Node. This Node is reserved.' followed by a list of properties for the 'OTHER' service level.

Properties	Custom Attributes 0	Members 0	Config Tracking	Templates 0	History
Cannot edit or delete this Node. This Node is reserved.					
Name:	OTHER				
Description:	Other service level				
Customer:	Customer Independent				
Operating System:	OS Independent				
Locked:	No				
Allow Servers:	Yes				
ID:	50003				

- 3** Click **Add**. The Service Levels page refreshes and the ADD SUB-NODE TO Service Levels form appears in the page.
- 4** Enter a name for the service level (required), and (optionally) enter notes and a description for the service level.

- 5 Click **Save**. The service level is added to the hierarchy of service levels. The Edit Service Level page appears, where you can change the properties of the service level, such as the customer association.

Editing a Service Level

Perform the following steps to edit a service level:

- 1 From the navigation panel, click Environment ► Service Levels. The Service Levels page appears.
- 2 Navigate the hierarchy of service levels until you reach the point in the hierarchy where you want to edit an existing service level.
- 3 Click **Edit** in the Properties tab. The page refreshes and an editable form appears for the service level properties.
- 4 Make changes to the service level name, description, notes, whether servers are allowed to be assigned to the service level, the associated customers and operating systems.
- 5 Click **Save**.

Ways to View the Service Level for Servers

Find the server whose service levels you want to view by searching or browsing the Manage Servers list.

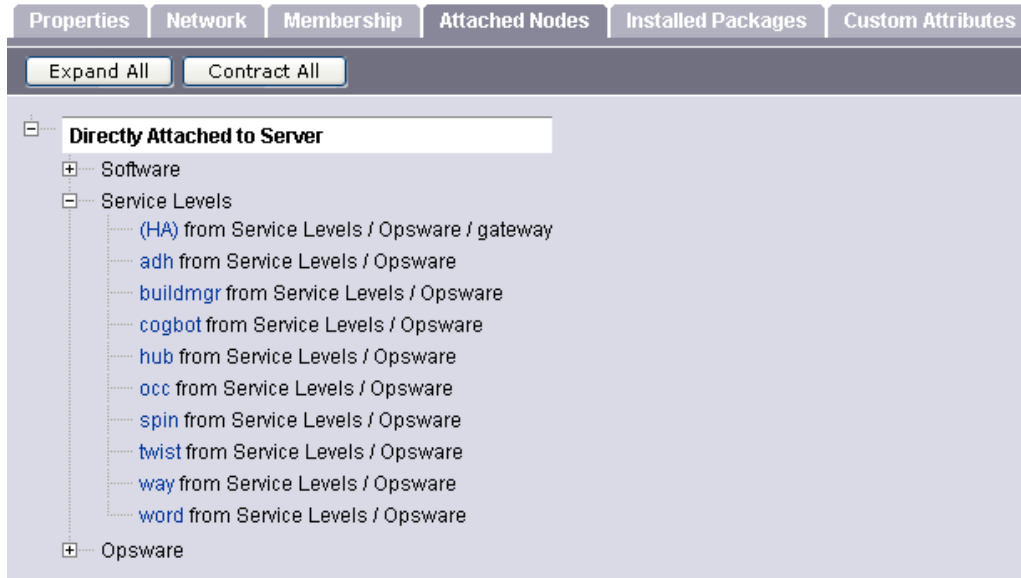
- If you are browsing the Manage Server list, you can find the service level for a server by locating the value in the Environment column, as Figure 8-20 shows.

Figure 8-20: Service Level Node Appearing in the Software Tab of the Server List

Managed Servers: Software View				
<input type="button" value="Ok"/> <input type="button" value="All Stages"/> <input type="button" value="All Uses"/> <input type="button" value="C06"/> <input type="button" value="Not Assigned"/> <input type="button" value="Update"/>				
Server	Software	Configuration Tracking	View	
<input type="checkbox"/>	Name	Hostname / IP Address	Software	Environment
<input type="checkbox"/>	ventoux.snv1.corp.opsware.com	ventoux.snv1.corp.opsware.com 192.168.9.79	OS: Red Hat Linux 7.3 / Not Assigned	Cust: Not Assigned Fac: C06 HW: DELL COMPUTER CORPORATION / PRECISION WORKSTATION 360 Rlm: Svc: Platinum Service

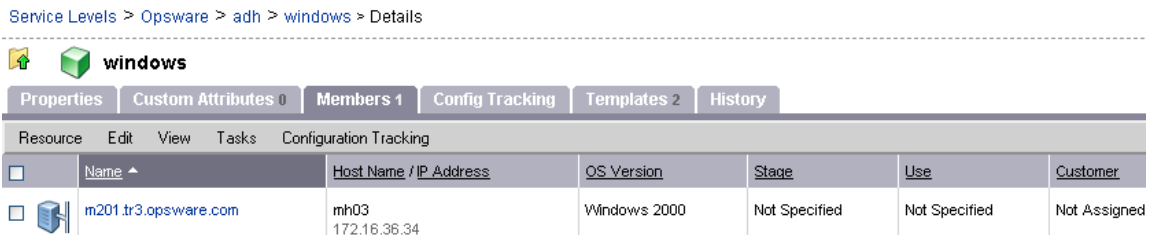
- If you searched for the server, click the server name and then select the Attached Nodes tab. You can find the service levels, as Figure 8-21 shows.

Figure 8-21: Nodes Tab That Shows the Service Level to Which a Server is Assigned



- To view all the servers assigned to a particular service level, click Environment ► Service Levels in the navigation panel. Navigate the hierarchy of service levels until you reach the one for which you want to see which servers are assigned. Select the Members tab, as Figure 8-22 shows.

Figure 8-22: Manage Server Assigned to a Service Level



Assigning a Server to a Service Level

Perform the following steps to assign a server to a service level:

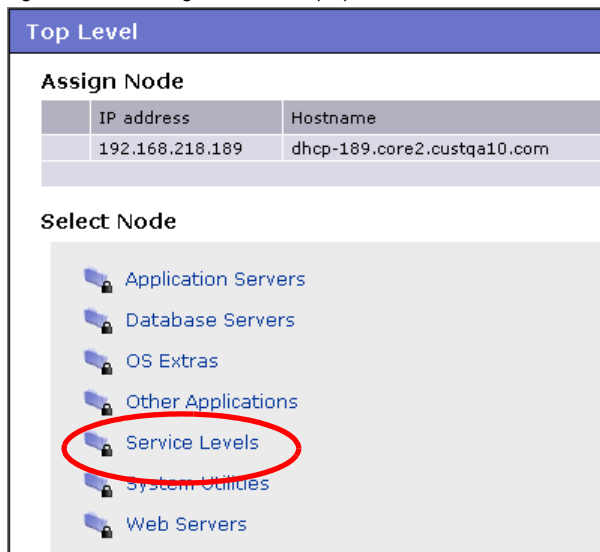
- 1 From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server you want to assign to a service level.

Or

Search for the server that you want to assign to a service level.

- 2** Select the servers that you want to assign to a service level.
- 3** Choose **Tasks ► Assign Node** from the menu above the Manage Servers list. A window displays the categories of nodes, as Figure 8-23 shows.

Figure 8-23: Assign Nodes Popup Window



- 4** Click the Service Levels link. The window refreshes to show the service levels created for your operational environment.
- 5** Navigate to the service level to which you want to assign the server.
- 6** Click **Assign**. The window closes and you are returned to the Manage Servers list.

Removing a Server from a Service Level

Perform the following steps to remove a server from a service level:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server that you want to remove from a service level.

Or

Search for the server that you want to remove from a service level.

- 2** Select the server that you want to remove from a service level.

- 3** Choose **Tasks** ► **Remove Node** from the menu above the Manage Servers list. A window displays the nodes to which the server is assigned, as Figure 8-24 shows.

Figure 8-24: Remove Nodes Popup Window

Nodes: Remove Nodes

List of Server

IP	Hostname
192.168.218.189 -	dhcp-189.core2.custqa10.com

Select the Nodes to Remove

Select	Node
1	Operating Systems / SunOS 5.8 / SunOS 5.8 - SUNWXCall
<input type="checkbox"/>	Service Levels / joe-constraint-test-SL

¹This Node Type cannot be removed. To change it, you must Re-Assign the Node.

Remove
Cancel

- 4** Select the service level node from which you want to remove the server and click **Remove**. You are prompted to confirm that you want to remove the server from the service level.

Click **Confirm Remove**. The window closes and you are returned to the Manage Servers list.

Network Configuration

This section provides information about network configuration within Opware SAS and contains the following topics:

- Overview of the Server Network Configuration
- Configuring Networking for an Opware Managed Server

Overview of the Server Network Configuration

You can use Opware SAS to automatically configure network settings for a server after you install the OS.

The OS Provisioning feature provisions servers with an OS by using DHCP addresses. Because DHCP servers often assign temporary IP addresses to servers that boot over a network, system administrators typically need to assign static IP addresses (and other

network properties) before the servers can be put into service. Opware SAS enables system administrators to do this through the SAS Web Client rather than logging onto the server manually after OS provisioning is complete.



Opware SAS does not support managed servers that have IPv6 addresses.

The Server Network Configuration feature allows you to configure the following settings on a server that are related to its network configuration:

- Host Name
- Domain Name System (DNS) servers
- Management interface (the interface that Opware SAS should use when managing the server)

See “Locating the Management IP Address of a Managed Server” on page 276 in Chapter 8 for more information.

- Gateway (the IP address of the default router)
- DNS search domains
- WINS (Windows Internet Naming Service) Servers
- Configuration for each network interface, including whether the interface is configured statically or with a Dynamic Host Configuration Protocol (DHCP) IP address, host name, and subnet mask

You can alter any of these options and then apply the settings to the managed server. Opware SAS updates the server and reboots it to cause the new settings to take effect.

Configuring Networking for an Opware Managed Server

You can only use the Network Configuration feature for servers running Sun Solaris, Red Hat Linux, and Microsoft Windows operating systems.

Perform the following steps to configure networking for an Opware managed server:

- 1** From the navigation panel, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server that you want to configure networking on.

Or

Search for the server that you want to configure networking on.

See “Using the Search Feature” on page 243 in Chapter 7 for more information. See “Server Searching by IP Address” on page 258 in Chapter 7 for more information.

- 2** Click the name of the server that you want to configure networking for. The Manage Servers: Properties page appears for that server.
- 3** Select the Network tab. The network information for the server displays.
- 4** Modify any of the following settings to configure the server networking.

For all fields, the default value is the one currently configured on the server.

- **Host Name:** The host name configured on the managed server. This field only sets the name by which the server knows itself and does not update DNS records for the server.
- **Management Interface:** Instructs Opsware SAS to use a particular network interface when contacting the server. This is useful, for example, when a server has multiple network interfaces, but not all of them are reachable by the Opsware core. Designating a particular interface as the management interface allows Opsware SAS to know which interface to use for managing the server.
- **Gateway:** The IP address of the default router
- **DNS Servers:** A list of DNS nameserver IP addresses
- **Search Domains:** A list of DNS domains to search when attempting to resolve host names
- **WINS Servers:** Set for Windows only; a list of WINS server IP addresses
- **Interface Configuration** (for each network interface in the system):
 - **DHCP:** If DHCP is enabled for an interface, the system uses DHCP to configure this network interface. In this case, static configuration settings (IP address, host name, and subnet mask) are not relevant for this interface, and the SAS Web Client makes those fields not editable. If DHCP is not enabled, then static settings are required.
 - **IP Address:** The IP address for this interface (unless DHCP is enabled).

- **Host Name:** The local host name for the server. This item is only required for servers running Solaris. Like the Computer Name field, this setting only affects the name by which the managed server knows itself, and does not update DNS records.
- **Subnet Mask:** The IP network mask to use for this interface.

In addition, Opware SAS displays the management IP address and MAC address for the server; however, you cannot change these values reported by the Opware Agent.

- 5** Click **Update Server** at the bottom of the page.

(If you click **Revert**, it causes any changes that you made to the fields to be discarded.)

A confirmation dialog box appears that shows the changes that will be made to the server. The confirmation dialog box includes a check box that allows you to indicate that the server should revert to its old network configuration when it cannot contact the Opware core after you save the new network configuration. By default, the Revert check box is selected.

The SAS Web Client does not validate the network configuration changes that you make in the Network tab. Therefore, it is possible to provide a malformed IP address in the IP address field for an interface.

- 6** To have the server revert to its previous network configuration if an error occurs, ensure that the check box is selected in the confirmation dialog box.
- 7** Click **OK** to proceed with the configuration changes.

A progress dialog box appears that shows the progress of the operation. The process of setting a new network configuration involves rebooting the managed server. The operation might take several minutes.

You can wait for the operation to complete or close the progress dialog box and perform other work in the SAS Web Client. The status of the task is available in the My Jobs user interface if you want to check the status of the network configuration update.

Details About Changing the Domain for Windows Servers

You cannot use the DNS Domain field to change the domain name for a Windows server.

Opware SAS does not change the domain name of a Windows server because changing the domain name of a server requires password authentication. Changing the domain name of a Windows server is a manual operation. See Figure 8-25.

Figure 8-25: DNS Domain Field Displays in the Network Tab for a Server

[Return to Manage Servers](#)

Properties	Network	Membership	Attached Nodes	Installed Packages	Custom Attributes	Config Tracking	History
NETWORK INFORMATION (as of Tue May 24 19:21:06 2005)							
Hostname:		<input type="text" value="core.tr3.opsware.com"/>					
Management IP:		<input type="text" value="172.16.36.18"/>					
Facility:		<input type="text" value="DATACENTER1"/>					
Management Interface:		<input type="text" value="eth0"/>					
Gateway:		<input type="text" value="172.16.36.17"/>					
DNS Servers:		<input type="text" value="66.54.32.78"/> <input type="text" value="66.54.0.78"/>					
Search Domains:		<input type="text" value="tr3.opsware.com"/> <input type="text" value="opsware.com"/>					

Chapter 9: NAS Integration

IN THIS CHAPTER

This section discusses the following topics:

- Overview of NAS Integration
- Device Information in SAS
- Device Groups
- Duplex Mismatch
- Network Device Information in NAS
- Network Reports

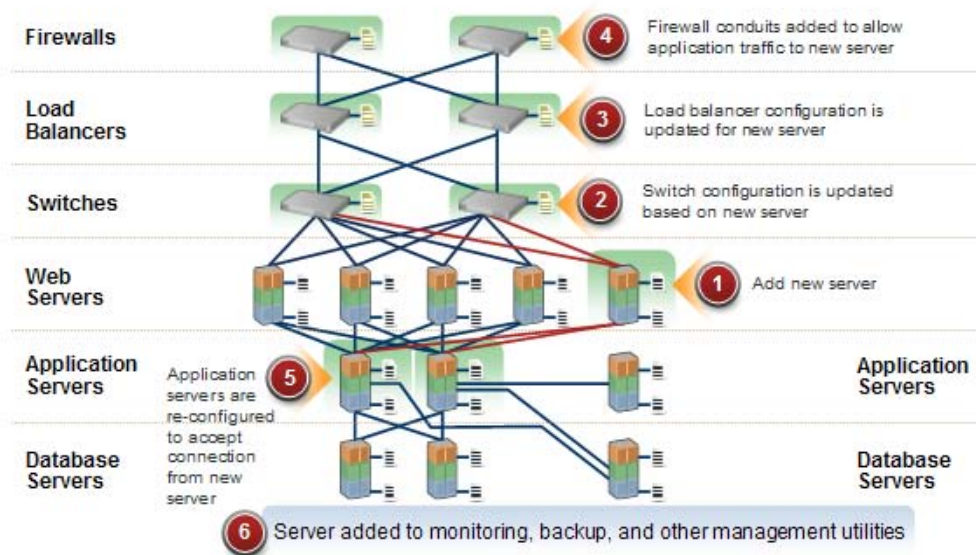
Overview of NAS Integration

Implementing changes in an IT environment often requires a coordinated effort between network administrators, system administrators, and application architects. Together, these members of the IT staff must manage an application environment spanning servers running different operating systems and network devices that include firewalls, load balancers, switches, servers, Web applications, and so on. For example, in some environments, you are required to make changes to network devices in front of an application, such as load balancers, firewalls, switches, and so on.

The NAS Integration feature makes this process easier. It enables IT staff members to see how servers are connected to network devices and enables them to closely examine managed servers. With this information, they can determine how all devices are related and coordinate and implement required changes.

Figure 9-1 shows the types of coordinated tasks you can perform by using the NAS Integration feature.

Figure 9-1: Overview of Coordinating Tasks Using NAS Integration



This section contains information about how to set up NAS Integration, view device details, examine connections between network devices and servers, identify duplex mismatches, and view combined device history information. It also contains information about implementing changes across the environment and generating network reports.

To support an integrated approach to making changes in your environment, such as server reallocation, ensuring compliance across servers and network devices, and detecting and resolving duplex mismatches, the NAS Integration feature provides the following Opsware interface points:

- Opsware Server Automation System (SAS)
- Opsware Network Automation System (NAS)
- Opsware Global Shell (in SAS)
- Opsware Visual Application Manager (in SAS)
- Opsware Reports (in SAS)

NAS Integration Features

In the NAS Integration feature, you will use several Opsware SAS and Opsware NAS features to perform the following tasks:

- Use SAS and NAS to view summarized and detailed hardware information about managed servers and network devices, and their connections (interfaces and ports).
- Use the Opsware Global File System (OGFS) to navigate between managed servers and connected network devices by tracing their associated physical connections, finding network device configurations, and running scripts across servers and network devices.
- Call NAS scripts from SAS scripts to automate operations across servers and network devices.
- Use features in SAS and NAS to create diagrams that illustrate managed servers, network devices, and layer 1 connections in your environment.
- Use SAS to identify, troubleshoot, and remediate configuration duplex mismatches between managed servers and network devices.
- Use SAS to perform actions on device groups that contain both servers and network devices.
- Use SAS to review a combined event history log of servers and network devices that records changes made to an application in your environment.
- Use SAS to export a combined event history log to a .csv file and an .html file.
- Use NAS to directly access additional network device details and event history.
- Use SAS to run network reports that identify layer 1 connections and configuration mismatches (duplex compliance).



Reference to *connections* in this documentation refer to *physical connections*, except where noted.

How NAS Data is Collected

The NAS Integration feature uses the NAS Topology Data Gathering and NAS Duplex Data Gathering diagnostic tools to collect information about network devices.

NAS Topology Data Gathering

The NAS Topology Data Gathering diagnostic instructs NAS to collect MAC addresses for all switches. MAC addresses are required to discover and add physical connections to the Opsware data model. For example, when you add another server to a switch, that information will be collected the next time the NAS Topology Data Gathering diagnostic runs. You can also run the NAS Topology Data Gathering diagnostic or the NAS Duplex Data Gathering on demand for specific network devices. See the *Opsware® NAS User's Guide*.

To avoid impairing performance in Opsware NAS, you cannot run this diagnostic any more frequently than weekly. If you cannot wait a week to refresh the NAS data, contact Opsware Support.

NAS Duplex Data Gathering

For network devices, speed and duplex is gathered by the NAS Duplex Data Gathering diagnostic, which runs after a device is initially added to NAS and then according to a schedule that you define. To ensure that you have the latest speed and duplex information about network devices, Opsware, Inc. recommends that you set up a recurring schedule that runs the diagnostic. See "Duplex Mismatch" on page 371 and the *Opsware® NAS User's Guide*.

Troubleshooting Tips

To test whether SAS is communicating with NAS, verify the following setup:

- Make sure you can log in to NAS with your SAS credentials. This ensures that NAS can communicate with SAS.
- Make sure the SAS credentials specified in the NAS Administrative Settings under External Authentication Type are set to Opsware Server Automation System. This ensures that NAS can look up server MAC addresses.
- Make sure the NAS Topology Gathering Diagnostic has run successfully by searching for tasks and check their results. This ensures that NAS has gathered MAC addresses and tried to look them up in SAS.

SAS Client Communication

Some NAS Integration features require that the SAS Client (Java) opens the NAS Web interface (directly from SAS) so that you can access additional details about certain NAS events. If you have completed the required setup tasks and the SAS Client is unable to communicate directly with the server running the NAS host (server) Web interface, you

might need to change the Opsware NAS option in the SAS Client. For example, if a firewall is preventing the SAS Client from reaching the NAS host, you need to specify the name of a server that is acting as a proxy for the NAS host. This will override the default setting.

This option enables you to specify the name of the NAS host that you log in to, restore the previously saved (default) host name, and launch the NAS login window to verify the host name.

To reset the Opsware NAS option, perform the following steps:

- 1** From the **Tools** menu in the Opsware Server Automation System window, select **Options**.
- 2** In the Views pane, select Opsware NAS.
- 3** In the Host field, enter the name of a server that is acting as a proxy for the NAS host, such as m208, which is the proxy for the m208.opsware.com NAS host.
- 4** (Optional) Click **Restore Default** to restore the previously saved NAS host name.
- 5** (Optional) Click **Test** to open the Opsware NAS login window.
- 6** Click **Save** to save your changes or click **Cancel** to close the window without saving your changes.

Prerequisites

The NAS Integration feature requires that both Opsware NAS 6.1 and Opsware SAS 6.0 are installed and configured to enable you to share data across servers and network devices in your environment. See the *Opsware[®] SAS Planning and Installation Guide*.

The Opsware Agent 6.0 is also required. If an Agent older than 6.0 is installed on a server, it cannot return the duplex and speed settings for the network interfaces. Therefore, duplex compliance cannot be calculated for that server.

Device Information in SAS

In addition to basic hardware details about managed servers and network devices, the NAS Integration feature also reports the following information about network interfaces and network ports:

- On the server side, network interfaces have the following properties: MAC address, subnet mask, interface type, IP address, DHCP setting, connected switch port, speed, and duplex (excluding Windows).

- On the network device side, network ports have the following properties: port name, speed and duplex settings, devices connected, and interface type.



For most devices, auto-negotiation works best when both sides of the connection (server and network device) are set to auto-negotiate mode. For example, a duplex policy could specify that a port should be set to full, half, or auto, and not to full (auto). A full (auto) duplex setting indicates that the port was set to auto-negotiate and it negotiated to full duplex. See the *Opsware® NAS User's Guide*.

The following tasks describe how you can access detailed hardware information for servers and network devices directly in Opsware SAS. See “Network Device Information in NAS” on page 369 for instructions on how to access hardware information about network devices directly in Opsware NAS.

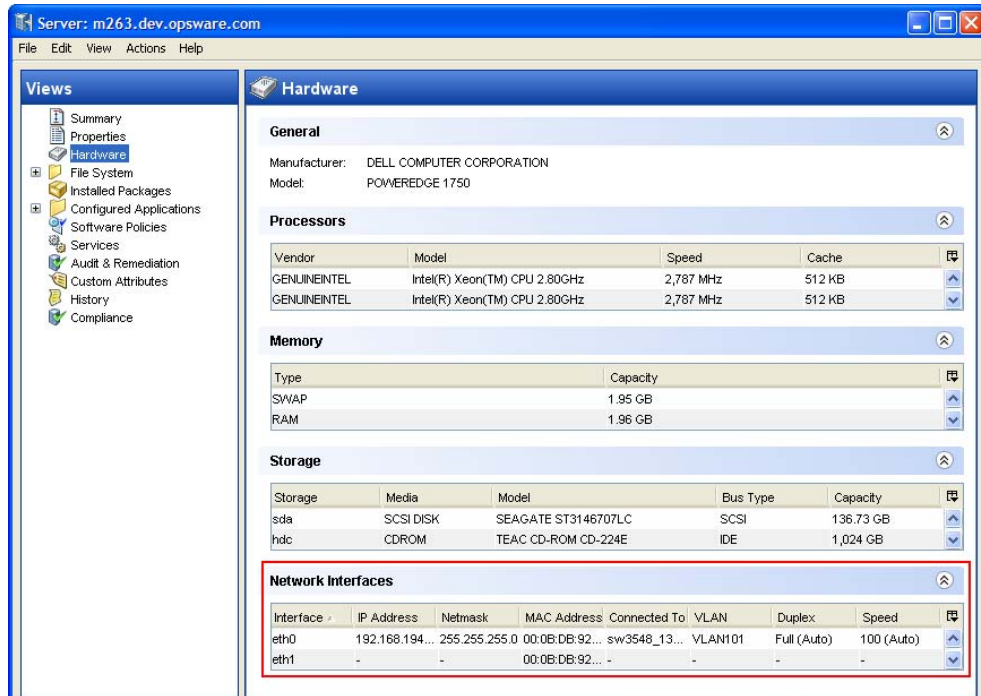
Viewing Network Interfaces

To view hardware information about a server, including network interfaces, perform the following steps:

- 1** From the Navigation pane, select Devices ► All Managed Servers.
- 2** From the View drop-down list, select Hardware.

- 3 Double-click on a server in the Content pane to display hardware details in the Server Explorer.

Figure 9-2: Hardware View in the Server Explorer



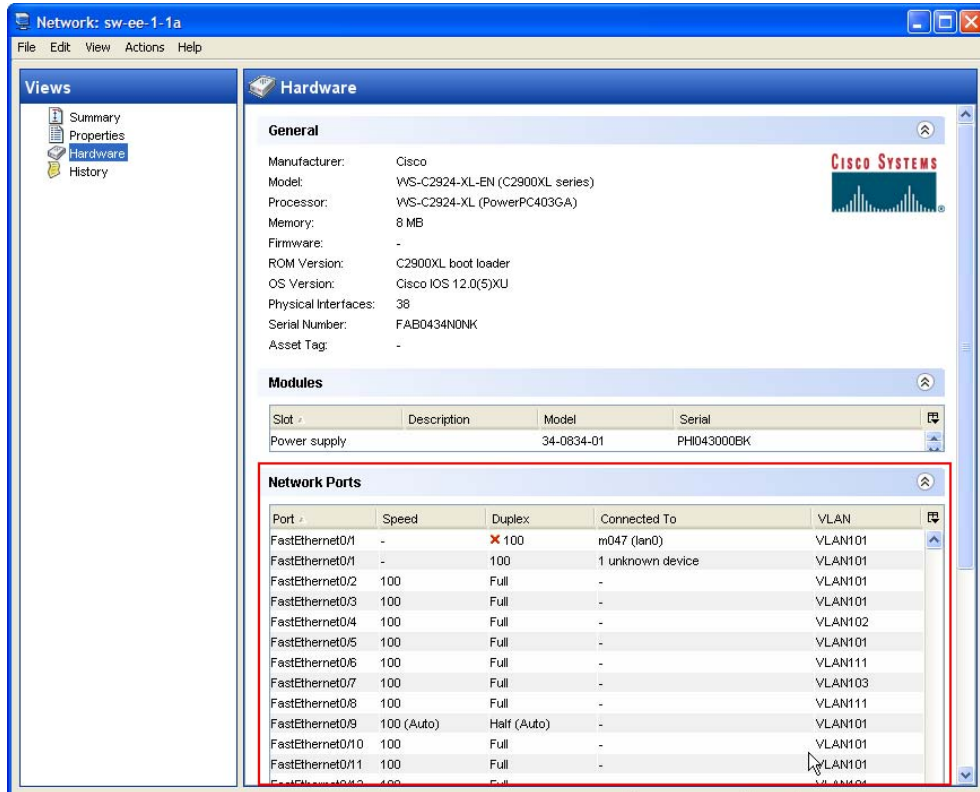
Viewing Network Ports

To view hardware information about a network device, including network ports, perform the following steps:

- 1 From the Navigation pane, select Devices ► Device Groups ► Public and then select a group.
- 2 Double-click on a network device in the Content pane to display the Network Device Explorer.

- 3 In the Views pane, select Hardware to display information about the selected network device.

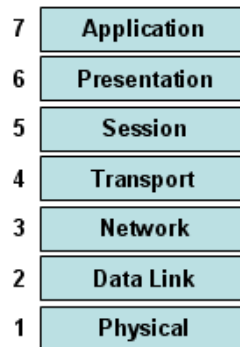
Figure 9-3: Hardware View in the Network Device Explorer



Connections Between Network Devices and Servers

The NAS Integration features are based on layer 2 connections and inferred layer 1 connections. See Figure 9-4 for definitions of the OSI Model layers.

Figure 9-4: OSI Seven Layer Model



Data Link Connections

The NAS Integration feature includes functionality that detects data link (layer 2) connections and reports on physical (layer 1) and data link connections. These data link connections include switches that are directly connected to a managed server and switches that are indirectly connected through other switches. These connections are discovered by correlating the MAC addresses reported by the device with the known MAC addresses for servers and switches.

Physical Connections

The physical connections are inferred from the data link connections. See “Inferred Physical Connections” on page 361. Physical connections represent direct connections (cables) between server and switches.

In the SAS Client, you can see physical connections in the Server Explorer, the Network Device Explorer and in detailed layout diagrams in the Visual Application Manager. In the NAS diagramming feature, you can see physical, data link or network (layer 3) connections.

Network Diagrams

You can use the Visual Application Manager feature in Opware SAS and the Diagramming feature in Opware NAS to create detailed diagrams that illustrate managed servers, network devices, and layer 2 and layer 1 connections in your environment. You can also export these network diagrams to .gif, .jpg, and .svg files, and then subsequently annotate and use them in other applications.

See the *Opware® SAS User's Guide: Application Automation* and the *Opware® NAS User's Guide* for more information about the Visual Application Manager and the Diagramming tool.

Launching Visual Application Manager

To access the Visual Application Manager, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **All Managed Servers**.
- 2** In the Content pane, select one or more servers.
- 3** From the **Tools** menu, select **Visual Application Manager** and then select one of the following options:
 - Select **New** to open the Opware Visual Application Manager window.
 - Select **Open** to open a previously saved topology.
- 4** To create and export topology diagrams, see the procedures for using Visual Application Manager in the *Opware® SAS User's Guide: Application Automation*.

Launching NAS Diagramming

See the *Opware® NAS User's Guide* for instructions on launching and using the Opware NAS Diagramming feature.

Network Directories

You can use the Global Shell feature to navigate between servers and connected network devices by tracing their physical connections in the `/opsw/Servers/@` and `/opsw/Network/@` directories in the OGFS.

You can also run three types of NAS scripts in the OGFS: command, advanced, and diagnostic. These scripts correspond to the three directories in the OGFS under `/opsw/Scripts/Network`. See "Network Directories" on page 577.

In the OGFS, you can also write scripts in languages, such as Bourne shell and Python, to perform the following tasks:

- Find servers and network devices.
- Find all servers that are connected to a certain switch.
- Find servers with a duplex mismatch.
- Display the network interfaces of a certain server.
- Get the IP addresses of all devices.
- Compare two files to identify changes in a network device's configuration.
- Change device details, such as the snmp-location.

Launching Global Shell

Within the Global Shell feature you can see all of the ports on a switch, view duplex settings in the info file, see all device configurations, compare configuration files, and so on. Every time a network device configuration is changed, a snapshot of it is also created. All actions that you perform on a device are audited.

To access the OGFS in the Global Shell feature, perform the following steps:

- 1** From the **Tools** menu, select **Global Shell** to launch a terminal window. See “Opening a Global Shell Session” on page 386.
- 2** To navigate between servers and connected network devices, use the guidelines described in “Global Shell” on page 375 and “OGFS Directories” on page 565.

Remote Terminal

The Remote Opsware Shell (`rosh`) utility enables you to log in to devices (servers and network devices) and run native commands. You invoke `rosh` from within a Global Shell session. You can run `rosh` and enter native commands interactively, or you can specify the native commands as an option of `rosh`. For example, you can log in to a switch with `rosh` and run the `show vlan` command to view all VLAN details.

See “Remote Terminal” on page 397 and “Logging on to a Managed Server With rosh” on page 390 for more information about using the `rosh` utility.

Inferred Physical Connections

The NAS Integration feature also includes functionality that detects and reports on inferred physical (layer 1) connections. These connections are inferred from data (such as MAC addresses that are seen by switches), captured, and then added to the Opsware data model.

These physical connections (inferred layer 1 data) are based on heuristics. In the OSI model, each layer is an abstraction designed to hide the layer below. Therefore, the layer 2 data gathered from devices cannot generate 100% accurate layer 1 data. In particular, layer 1 data may be incorrect if any of the following conditions exist:

- The device does not return the port number where MAC addresses are seen.
- There was no traffic between the devices within a few minutes of when NAS gathered the topology data (where MAC addresses are seen).
- There is an unmanaged device between two managed devices.
- There is a hub between two managed devices.

In the SAS Client, you can see inferred layer 1 connections by navigating network device directories in Opsware Global Shell .

Device Groups

A device group helps you categorize your devices (servers and network devices) in ways that make sense for your organization. For example, you can group devices by customer, facility, usage, application, and so on, and then perform actions on all of the devices in the group.

In SAS, a device group can contain managed servers *and* network devices, or *only* managed servers. In Opsware NAS, a device group contains only network devices. You create and edit network device groups only in NAS. See the *Opsware® NAS User's Guide* for more information about using the `rosh` utility.

The NAS Integration feature allows you to associate a public device group (that exists in Opsware SAS) with a device group (that exists in Opsware NAS). The device group names must be identical and you must enable the corresponding option. To monitor an application that is running on multiple servers and relies on multiple network devices in your environment, Opsware, Inc. recommends that you model it as a device group that contains all servers and network devices the application runs on. This enables you to troubleshoot the application by using SAS.

Associating a NAS Device Group

When you associate a public device group in SAS with a device group in NAS, you will be able to monitor information about all servers and network devices that you are interested in. You associate device groups by using identical group names.

To associate device groups in SAS and NAS, perform the following steps:

- 1** From the Navigation pane, select **Devices** ► **Device Groups** ► **Public**.
- 2** In the Content pane, select a device group.
- 3** Right-click on the device group and then select **Open** to display the Device Group Explorer.
- 4** From the View drop-down list, select **Properties**.
- 5** Check the “Associate with a NAS device group of the same name” check box to enable this functionality.
- 6** From the **File** menu, select **Save**.

Combined Device History Log

The combined device history log records events performed on servers and network devices in your environment. These events are recorded in detail as actions performed on a certain date, by a certain user, on a certain server, or on a certain network device.

In many troubleshooting tasks, this type of information is critical because some of these actions (changes) might be the root cause of problems. This log provides detailed information, such as the date the action occurred, the name and type of the device that the action was performed on, and a description of the action, that can help you perform root cause analysis, capacity planning, and compliance remediation tasks. For example, if an application in your environment has suddenly stopped running and you know exactly when it was previously running, you need to examine a combined event history log for the affected servers and network devices, for that time period. This information can help you determine why the application stopped working.

Viewing a Combined Device Event History Log

You can view a detailed list of events that occurred on a server or network device, such as all changes made to an application. You can narrow the time frame of the log display to see changes that occurred daily, weekly, monthly, quarterly, or in a custom range of dates. You can also dynamically filter the display of events by a certain date, device name, device type, event type, or by user name.

You can view a combined device history log for one or more managed servers or for a device group that contains managed servers and network devices.

To view a combined device history log for a device group, perform the following steps:

- 1 From the Navigation pane, select Devices ► Device Group, and then select a device group.
- 2 In the Content pane, select one or more devices in the group.
- 3 Right-click and then select View History to list events that occurred on the selected devices.

Figure 9-5: Combined Device Event History

Date	Device Name	Device Type	Event	User
Mon Jun 26 04:...	im106.pr5.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 04:...	im101.pr5.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515..."	cstarkey
Mon Jun 26 04:...	im105.pr5.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515..."	cstarkey
Mon Jun 26 04:...	im101.pr5.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515..."	cstarkey
Mon Jun 26 04:...	im105.pr5.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	im105.pr5.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 04:...	im101.pr5.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 04:...	im106.pr5.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515..."	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	cstarkey
Mon Jun 26 04:...	co140.pr5.ops...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	cstarkey
Mon Jun 26 01:...	sw1.pr5	Switch	Task Started	admin
Mon Jun 26 01:...	sw1.pr5	Switch	Last Used Device Password Changed	-
Mon Jun 26 01:...	sw1.pr5	Switch	Device Diagnostic Completed Successfully	admin
Mon Jun 26 01:...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 22:0...	sw1.pr5	Switch	Device Snapshot	admin
Sun Jun 25 22:0...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 22:0...	sw1.pr5	Switch	Last Used Device Password Changed	-
Sun Jun 25 22:0...	sw1.pr5	Switch	Task Started	admin
Sun Jun 25 19:0...	sw1.pr5	Switch	Task Started	admin
Sun Jun 25 19:0...	sw1.pr5	Switch	Last Used Device Password Changed	-
Sun Jun 25 19:0...	sw1.pr5	Switch	Device Diagnostic Completed Successfully	admin
Sun Jun 25 19:0...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 16:0...	sw1.pr5	Switch	Device Snapshot	admin
Sun Jun 25 16:0...	sw1.pr5	Switch	Task Completed	admin
Sun Jun 25 16:0...	sw1.pr5	Switch	Last Used Device Password Changed	-

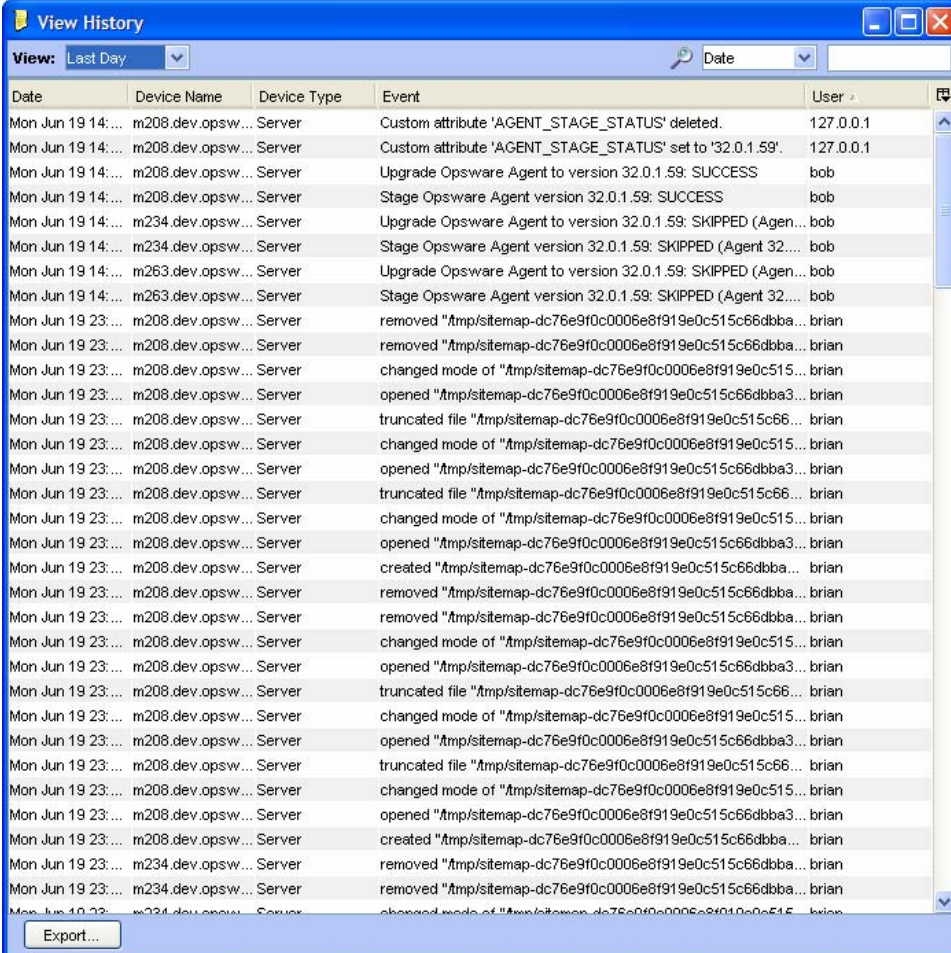
Viewing an Event History Log for Servers

To view a combined device history log for one or more managed servers, perform the following steps:


- 1 From the Navigation pane, select Devices ► All Managed Servers.

- 2 In the Content pane, select one or more servers.
- 3 Right-click and then select View History to list events that occurred on the selected servers.

Figure 9-6: View History of Servers

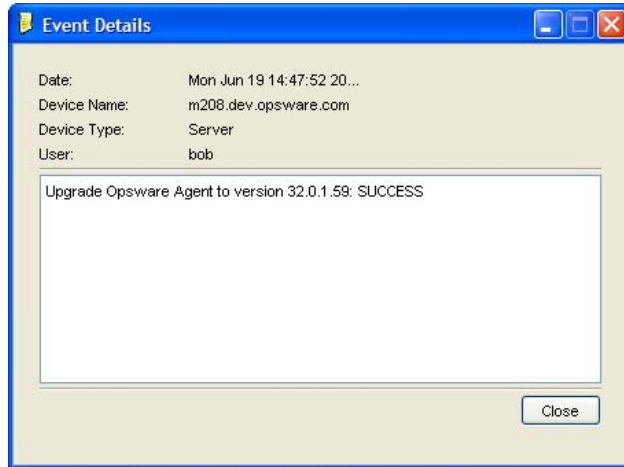


Date	Device Name	Device Type	Event	User
Mon Jun 19 14:...	m208.dev.opsw...	Server	Custom attribute 'AGENT_STAGE_STATUS' deleted.	127.0.0.1
Mon Jun 19 14:...	m208.dev.opsw...	Server	Custom attribute 'AGENT_STAGE_STATUS' set to '32.0.1.59'.	127.0.0.1
Mon Jun 19 14:...	m208.dev.opsw...	Server	Upgrade Opsware Agent to version 32.0.1.59: SUCCESS	bob
Mon Jun 19 14:...	m208.dev.opsw...	Server	Stage Opsware Agent version 32.0.1.59: SUCCESS	bob
Mon Jun 19 14:...	m234.dev.opsw...	Server	Upgrade Opsware Agent to version 32.0.1.59: SKIPPED (Agen...	bob
Mon Jun 19 14:...	m234.dev.opsw...	Server	Stage Opsware Agent version 32.0.1.59: SKIPPED (Agent 32....	bob
Mon Jun 19 14:...	m263.dev.opsw...	Server	Upgrade Opsware Agent to version 32.0.1.59: SKIPPED (Agen...	bob
Mon Jun 19 14:...	m263.dev.opsw...	Server	Stage Opsware Agent version 32.0.1.59: SKIPPED (Agent 32....	bob
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba3...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	truncated file "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	opened "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m208.dev.opsw...	Server	created "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m234.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m234.dev.opsw...	Server	removed "/tmp/sitemap-dc76e9f0c0006e8f919e0c515c66dbba...	brian
Mon Jun 19 23:...	m234.dev.opsw...	Server	changed mode of "/tmp/sitemap-dc76e9f0c0006e8f919e0c515...	brian

- 4 (Optional) In the View History window, select an option in the View drop-down list to list events by a time period, such as Last Day, Last Week, Last Month, or Custom Range.
- 5 (Optional) In the View History window, use the search tool  to dynamically filter the display of events by a certain date, device name, device type, event type, or by user name.

- 6** (Optional) To identify the device name and type for a certain event, double-click on the event listed in the View History window to display the Event Details window.

Figure 9-7: Event Details for a Selected Server




To view the combined device history log for a device group, perform the following steps:

- 1** From the Navigation pane, select Devices ► Public.
- 2** In the Content pane, select one or more devices in the group.

- 3 Right-click and then select View History to list events that occurred on the selected network devices.

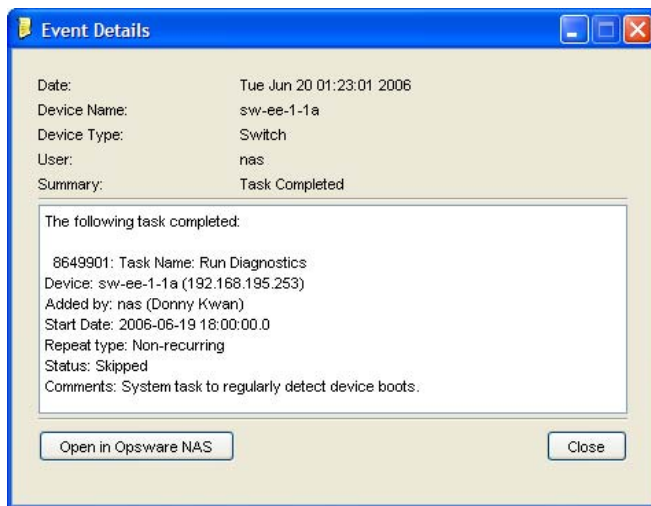
Figure 9-8: View History of Network Devices

Date	Device Name	Device Type	Event	User
Mon Jun 26 20:...	sw-ee-1-1a	Switch	Device Snapshot	-
Mon Jun 26 20:...	sw-ee-1-1a	Switch	Task Completed	-
Mon Jun 26 20:...	sw-ee-1-2a	Switch	Device Snapshot	-
Mon Jun 26 20:...	sw-ee-1-2a	Switch	Task Completed	-
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Device Snapshot	-
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Task Completed	-
Mon Jun 26 20:...	sw-ee-1-1a	Switch	Task Started	-
Mon Jun 26 20:...	sw-ee-1-2a	Switch	Task Started	-
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Task Started	-
Mon Jun 26 20:...	sw-ee-1-1a	Switch	Session Data Captured	eslatis
Mon Jun 26 20:...	sw-ee-1-2a	Switch	Session Data Captured	eslatis
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Session Data Captured	eslatis
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Device Snapshot	-
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Task Completed	-
Mon Jun 26 20:...	sw-ee-1-2b	L3Switch	Task Started	-
Mon Jun 26 19:...	sw-ee-1-1a	Switch	Device Snapshot	-
Mon Jun 26 19:...	sw-ee-1-1a	Switch	Task Completed	-
Mon Jun 26 19:...	sw-ee-1-2a	Switch	Device Snapshot	-
Mon Jun 26 19:...	sw-ee-1-2a	Switch	Task Completed	-
Mon Jun 26 19:...	sw-ee-1-1a	Switch	Task Started	-
Mon Jun 26 19:...	sw-ee-1-2a	Switch	Task Started	-
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Session Data Captured	psi
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Device Snapshot	-
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Task Completed	-
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Task Started	-
Mon Jun 26 19:...	sw-ee-1-2a	Switch	Session Data Captured	eslatis
Mon Jun 26 19:...	sw-ee-1-1a	Switch	Session Data Captured	eslatis
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Session Data Captured	psi
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Device Snapshot	-
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Task Completed	-
Mon Jun 26 19:...	sw-ee-1-2b	L3Switch	Task Started	-

- 4 (Optional) In the View History window, select an option in the View drop-down list to list events by a time period, such as Last Day, Last Week, Last Month, or Custom Range.
- 5 (Optional) In the View History window, use the search tool  to dynamically filter the display of events by a certain date, device name, device type, event type, or by user name.

- 6 (Optional) To display details for a certain event, double-click on the event listed in the View History window to display the Event Details window.

Figure 9-9: Event Details for a Selected Network Device



Exporting a Combined Device History Log

If you need to use the log file in different applications, you can export the list of combined device history events to a .csv or an .html file.

To export the combined device history log, perform the following steps:

- 1 From the View History window, click **Export** to display the Export Dashboard window.
- 2 In the Look in field, enter the location of where you want to save the file.
- 3 (Optional) From the Encoding drop-down list, select a character encoding option. The default is Unicode (UTF-8).
- 4 In the File name field, enter a name for the file.
- 5 In the Files of type field, select .csv or .html.
- 6 Click **Export** to save the file in the selected format or click **Cancel** to close this window without saving.

Network Device Information in NAS

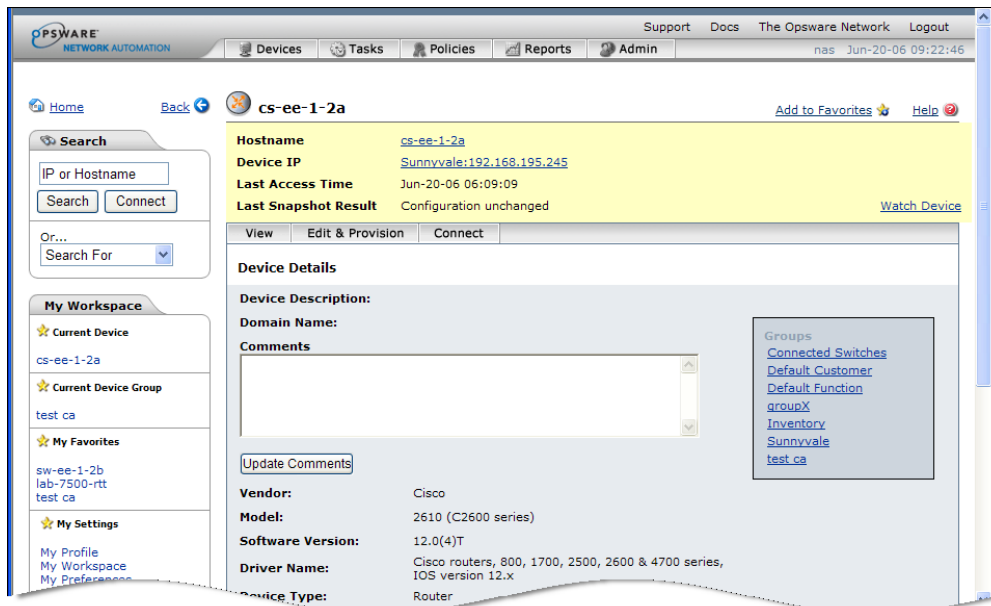
To help you with troubleshooting tasks that involve network devices in your environment, you can examine additional network device details and network device event history by logging directly in to Opware NAS. The NAS Integration feature provides a login option to access detailed information about network devices and their event history as recorded in Opware NAS.

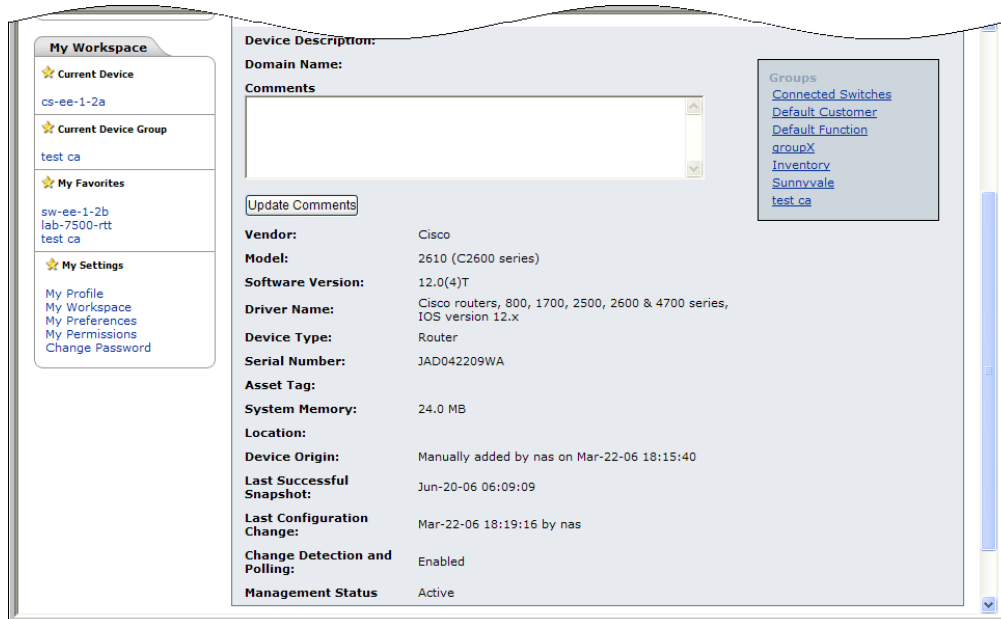
Viewing a Network Device Directly in Opware NAS

If you want to view detailed information about a network device directly in Opware NAS, perform the following steps:

- 1 From the Navigation pane, select **Devices** ► **Device Group** ► **Public**.
- 2 In the Content pane, select a network device.
- 3 Right-click and select **Open in Opware NAS** to display the Opware NAS login window.
- 4 Enter your user name and login, and then click **Login** to display device details in NAS.

Figure 9-10: Network Device Details in NAS





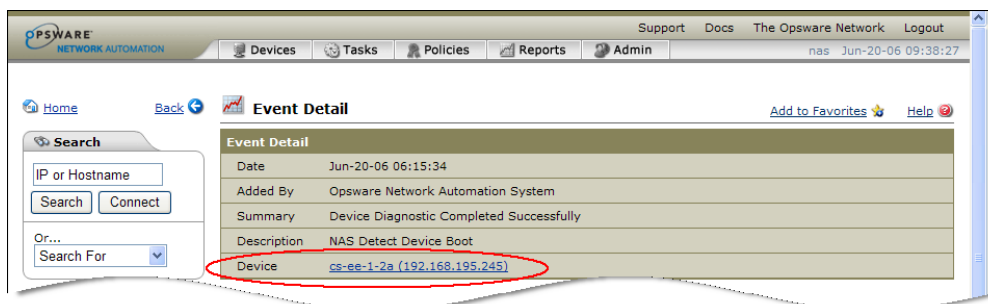
- 5 Click **Logout** to exit NAS.

Viewing Event History Directly in Opware NAS

If you want to view event details directly in Opware NAS, perform the following steps:

- 1 In the Event Details window, click **Open in Opware NAS** to display the Opware NAS login window. See Figure 9-8 on page 367.
- 2 Enter your user name and login, and then click **Login** to display event details in NAS.

Figure 9-11: Event Details for a Network Device in NAS



- 3 Click on the Device link to view additional information, such as timestamps for when the device was added, the last snapshot, and the last configuration change. See Figure 9-9 on page 368.
- 4 Click **Logout** to exit NAS.

Duplex Mismatch

The NAS Integration feature provides automatic detection of duplex mismatches. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.

For servers' network interfaces, speed and duplex information is gathered during every hardware registration, which occurs every 24 hours. See "Opware Agent Management" on page 99 for information about hardware registration.

Due to the lack of a device independent method of determining duplex for servers running a Windows operating system, the Opware Agent for Windows does not report duplex settings out-of-the-box. A custom script can be added to the Opware Agent to collect and report the speed and duplex setting for a certain network interface. For instructions on how to create and integrate the script with the Agent, contact Opware Support.

Speed and duplex information for servers is *not* updated when you select **View** ► **Refresh** or press F5 in the SAS Client. This data gets updated when the NAS Duplex Data Gathering diagnostic runs. See "NAS Duplex Data Gathering" on page 354.

For network devices, speed and duplex is gathered by the NAS Duplex Data Gathering diagnostic, which runs according to a schedule that you define. To ensure that you have the latest speed and duplex information about network devices, Opware, Inc. recommends that you set up a recurring schedule that runs the diagnostic. See the *Opware® NAS User's Guide*.

If the network interface information (speed and duplex) for a server does not match the network port information (speed and duplex) for a connected network device, it is considered to be non-compliant.


In the NAS Integration feature, you can see duplex mismatches identified at a top level by using the Dashboard. You can also see duplex mismatches identified by server and network device by using the Server Explorer and Network Device Explorer, respectively.

Viewing Duplex Mismatches in the Dashboard

See the *Opware® SAS User's Guide: Application Automation* for information about duplex compliance levels and how they are displayed in the Dashboard.


Viewing Duplex Mismatches by Server

To view duplex mismatches using the Server Explorer, perform the following steps:

- 1** From the Navigation pane, select Devices ► All Managed Servers.
- 2** In the Content pane, select a server.
- 3** Double-click on the server to display the Server Explorer.
- 4** In the Views pane, select Hardware.
- 5** In the Network Interfaces section, review the Duplex column for detected mismatches. Mismatches are identified by an  icon that precedes the duplex setting (Full, Half, Auto), in the Duplex column.

Viewing Duplex Mismatches by Network Device

To view duplex mismatches using the Network Device Explorer, perform the following steps:

- 1** From the Navigation pane, select Devices ► Device Groups ► Public.
- 2** In the Content pane, select a network device.
- 3** Double-click on the network device to display the Network Device Explorer.
- 4** In the Views pane, select Hardware.
- 5** In the Network Ports section, review the Duplex column for detected mismatches. Mismatches are identified by an  icon that precedes the duplex setting (Full, Half, Auto), in the Duplex column. See Figure 9-2 on page 357.

Network Reports

To help troubleshoot problems that involve physical connections and duplex compliance, you can run and examine several network reports. By using the Reports feature in the SAS Client, you can produce the following network reports that identify layer 1 connections and configuration mismatches (duplex compliance) between managed servers and network devices in your environment:

Connections by Network Device

This report lists all physical connections to a selected network device.

Connections by Server

This report lists all physical connections to a selected managed server.

Duplex Compliance (All Servers)

This report groups all managed servers by duplex compliance level to show configuration mismatches between servers and network devices. Click on a section of the chart to display a list of servers in a certain compliance level. Double-click on a server for more details or to perform an action.

Duplex Compliance by Customer

This report lists all managed servers by customer and then by duplex compliance level to show configuration mismatches between servers and network devices. Double-click on a server for more details or to perform an action.

Duplex Compliance by Facility

This report lists all managed servers by facility and then by duplex compliance level to show configuration mismatches between servers and network devices. Click on a section of the chart to display a list of servers in a facility with a certain compliance level. Double-click on a server for more details or to perform an action.



See “Reports” in the *Opware[®] SAS User’s Guide: Application Automation* for information about how to run, export, and print these reports.

Chapter 10: Global Shell

IN THIS CHAPTER

This section discusses the following topics:

- Overview of the Global Shell
- Global Shell Tutorial
- Global Shell Examples
- Character Encoding for the OGFS
- Global Shell Error Messages
- Remote Terminal

Overview of the Global Shell

The Global Shell is a command-line interface to the Opware Global File System (OGFS). The command-line interface is a Unix shell such as `bash` that runs in a terminal window. The OGFS unifies the Opware data model and the contents of managed servers, including files, into a single, virtual file system. You open a Global Shell session from within the SAS Client or from a direct `ssh` connection in a terminal client on your desktop. With the Global Shell, you can automate repetitive system administration tasks by running scripts across multiple servers in a secure environment.

Opware Global File System (OGFS)

The OGFS represents the Opware data model as a hierarchical structure of file directories and text files. For example, in the OGFS, the `/opsw/Customers` directory contains details about Opware customers and the `/opsw/Server` directory has information about managed servers. The `/opsw/Server` directory also contains subdirectories that reflect the contents (such as file systems and registries) of the managed servers. If you have the required permissions, in the Global Shell, you can view and even modify the file systems of managed servers.

Remote Opware Shell (rosh) Utility

The Remote Opware Shell (`rosh`) utility enables you to log on to managed servers and run native commands. You invoke `rosh` from within a Global Shell session. You can run `rosh` and enter native commands interactively, or you can specify the native commands as an option of `rosh`.

Benefits of the Global Shell

The Global Shell, OGFS, and `rosh` utility, offer the following benefits:

- **Security:** Logging on to managed servers is controlled by the Opware SAS security framework.
- **Auditing:** Logins and commands on managed servers are recorded in audit log files.
- **Re-use of existing scripts:** Existing native scripts can run on managed servers with the `rosh` utility. For example, you can run `.BAT`, `.vbs`, and `.sh` scripts on managed servers. Scripts written in Unix shells will run within the Global Shell, which supports `bash`, `csh`, and other common shells.
- **Routine maintenance tasks on multiple servers:** By accessing the global view of the OGFS, system administration scripts can run iteratively on groups of servers.
- **Access to the Opware SAS data model:** Global shell scripts can access information about managed servers, including custom attributes.

Commands Available in the Global Shell

The Global Shell offers the following types of Unix shells:

```
bash (default)
csh
ksh
sh
tcsh
```

Many common Unix commands (too numerous to list here) are available within the Global Shell. To display these commands, in a Global Shell session, list (`ls`) the contents of the following directories:

```
/bin /usr/bin
/opsw/bin
```

The `/opsw/bin` directory contains utilities (such as `rosh`) which are specific to Opware SAS. For more information, see "Global Shell Utilities Syntax" on page 553.

Differences Between the Global Shell and Unix Shells

The Global Shell is different from native Unix shells in the following ways:

- **Restricted command set:** Some Unix commands (such as `cron`) are unavailable in the Global Shell. To find out if a command is available, use the `which` command.
- **Limited recursion:** Commands cannot use recursion with the file systems of managed servers. Examples of recursive commands are `find`, `ls -r`, and `rm -r`.
- **Opware user:** You log on to the Global Shell as an Opware user, not as a Unix user.
- **Opware permissions:** The operations that you can perform and the servers that you can access are limited by the Opware permissions of your Opware user group.
- **Private directories:** The following directories are accessible only by your Opware user:

```
/tmp
/var/tmp
/usr/tmp
```

For example, the `/tmp` directory seen by the `jdoe` Opware user is different than the `/tmp` seen by `tjones`.

- **Opware data model in the OGFS:** Stored in the Opware Model Repository, the data model consists of objects such as customers, facilities, and servers. End users manipulate these objects with the SAS Client. The OGFS represents the data model in a file system that resembles a Unix file system. Changes to the data model appear as changes in the OGFS, and vice versa.
- **Axis (@) symbol in directory names:** In the OGFS, for example, this symbol appears in the following directories:

```
/opsw/Server/@
/opsw/Server/@Group
/opsw/Group/Public/group-name/@
```

The axis (@) symbol represents the end of the filtering criteria for managed servers.

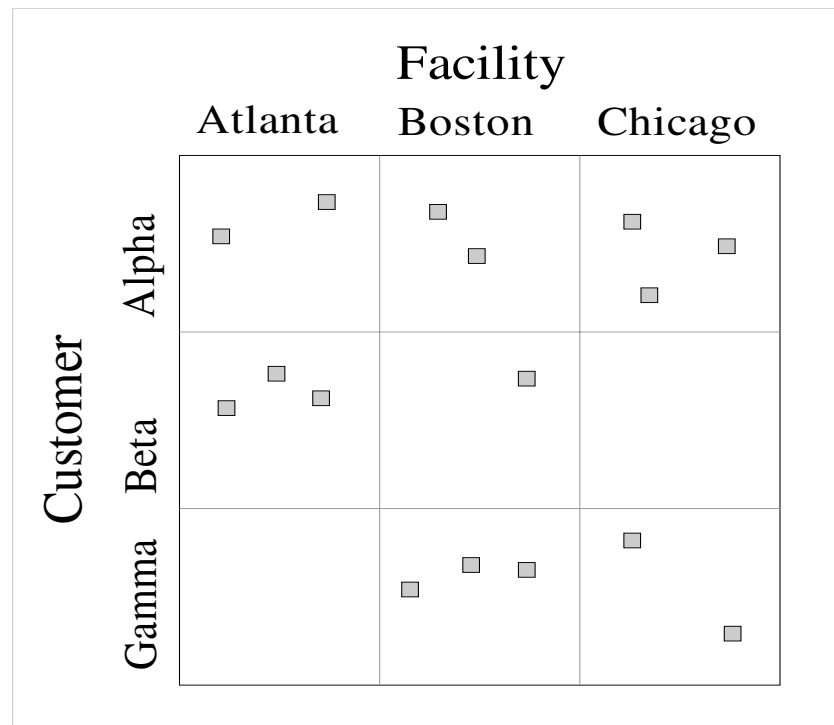
Server Filtering in the OGFS

As you navigate down the OGFS tree, the path grows longer and more specific as fewer servers are visible in the `Server` directory. In the OGFS, the `/opsw` directory contains subdirectories for several types of objects in the Opware model space, such as `Server`, `Group`, `Facility`, `OS`, `Application`, `Customer`, and so on.

In the Global Shell interface, you can filter your view of these object types in the `Server` directory by specifying an axis (@) in the path. A path in the Opsware model space can be a list of filtering criteria that selects objects of a given type. This path begins with the desired object type, such as `/Server`, and each filtering criteria begins with an @, such as `@Customer`. An ending @ denotes the end of the filtering criteria.

Figure 10-1 is graphical representation of related objects (customers and facilities) in a hierarchical `Server` directory. The small boxes represent managed servers. Examples of ways that you can filter this directory immediately follow the diagram.

Figure 10-1: Filtering in the Server Directory



Based on Figure 10-1, the following examples illustrate ways to narrow your search for servers:

- To find all 16 servers, specify the following path:

```
ls /opsw/Server/@
```

- To find servers in the Atlanta facility, specify the following path:

```
ls /opsw/Server/@Facility/Atlanta/@
```

- To find servers that belong to customer Alpha, specify the following path:

```
$ ls /opsw/Server/@Customer/Alpha/@
```

- To find servers in the Atlanta facility that belong to customer Alpha, specify either of the following paths:

```
ls /opsw/Server/@Facility/Atlanta/@Customer/Alpha/@
ls /opsw/Server/@Customer/Alpha/@Facility/Atlanta/@
```

The following paths are filtered away by the OGFS, because they would yield a dead-end. There are no servers belonging to customer Gamma in the Atlanta facility.

```
ls /opsw/Server/@Facility/Atlanta/@Customer/Gamma/@
ls /opsw/Server/@Customer/Gamma/@Facility/Atlanta/@
```



This same filtering logic can be applied to @Realm, @Group, and @Application.

Global Shell Tutorial

This tutorial covers just a few of the highlights of the OGFS and the Global Shell. After completing this tutorial, you will know how to navigate the directories of the OGFS and how to run commands on managed servers from within the Global Shell. Although the tutorial is organized into steps, after performing step 1, you can perform the remaining steps in any order.

Before starting the tutorial, you need the following capabilities:

- You can log on to the SAS Client. As you work through this tutorial, you might find it helpful to compare the stdout of the Global Shell with information displayed by the SAS Client.
- Your Opware user has Read & Write permissions on at least one managed server. Typically assigned by a security administrator, permissions are discussed in the *Opware® SAS Administration Guide*.
- Your Opware user has all Global Shell permissions on the same managed server. For information on these permissions, see “aaa Utility” on page 553.

The example commands in this tutorial operate on a Windows server named `abc.opsware.com`. This server belongs to a device group named All Windows Servers. When trying out these commands, substitute `abc.opsware.com` with the host name of

the managed server you have permission to access. Also, replace `jdoe` with your Opware user name. If you wish to run the commands on a Unix managed server, replace `ipconfig` with `ifconfig`; and replace `Administrator` with `root`.

Now, let's get started with the tutorial:

1 Open a Global Shell session.

You can open a Global Shell session from within the SAS Client. From the **Actions** menu, select **Global Shell**. You can also open a Global Shell session from a terminal client running on your desk top. For instructions, see "Opening a Global Shell Session" on page 386.

2 Check your session.

First, enter the `whoami` command, which displays the Opware user name for this session:

```
$ whoami
jdoe
```

You can enter the `ps` command to view the process status of your Global Shell session. The following `ps` command shows the session is running the default `bash` shell:

```
$ ps
PID TTY          TIME CMD
 7033 ?             00:00:00 bash
13712 ?             00:00:00 ps
```

Enter the `uname` command, which displays information about the server running the OGFS component of Opware SAS:

```
$ uname -a
Linux m171.dev.opsware.com 2.4.21-32.ELsmp #1 SMP Fri Apr 15
21:17:59 EDT 20 05 i686 GNU/Linux
```

If you log on to a Unix managed server with `rosh`, `uname` displays information about that managed server, not the server running the OGFS component. Run the `uname` command when you are not sure if you are interacting with the Global Shell or with the shell of a managed server accessed with `rosh`.

3 Confirm your home directory.

Every Opsware user has a home directory in the OGFS. The home directory has a `public/bin` subdirectory where you can store scripts to be executed by other users running Global Shell sessions. Each Opsware user also has a personal `/tmp` directory for temporary files. You cannot view or modify the `/tmp` directories of other users.

The following commands show some information about the directories of the `jdoe` user:

```
$ cd
$ pwd
/home/jdoe
$ ls -ld /home/jdoe/public/bin
drwxr-xr-x 2 jdoe jdoe 4096 2006-05-17 17:12 /home/jdoe/
public/bin
$ ls -ld /tmp
drwxrwxrwx 3 root root 4096 2006-06-09 23:37 /tmp
```

4 List all managed servers.

The `/opsw/Server` directory of the OGFS contains information about the servers managed by Opsware SAS. This directory is an example of how the OGFS represents objects (in this case servers) of the Opsware SAS data model. Behind the scenes, Opsware SAS stores this information in a database referred to as the Model Repository.

To view the names of the servers managed by Opsware SAS, enter the following command:

```
$ ls /opsw/Server/@
abc.opsware.com      m33.opsware.com      gist.opsware.com
pal.opsware.com      hare.opsware.com      qv55.opsware.com
. . .
```

5 Examine server information.

Each managed server has a directory structure containing information about that server. The `attr` subdirectory contains text files that describe the server's attributes. The attribute name matches the file name and the attribute value is the file contents. The following `cat` command lists the OS version of the managed server named `abc.opsware.com`:

```
$ cd /opsw/Server/@/abc.opsware.com
$ cat attr/osVersion
Microsoft Windows 2000 Advanced Server Service Pack 4 Build
2195 (05-02-2006)
```

The `Interface` subdirectory has information about the server's network interfaces. Here's an example:

```
$ cat "Interface/Local Area Connection/info"
AdminEnabledFlg: no
CardIndex:
CardSerialNum:
CircuitId:
Collisions:
ConfiguredDuplex: AUTO
ConfiguredSpeed: AUTO
. . .
```

6 List the files of a managed server.

In addition to information about managed servers, `/opsw/Server` contains directories that correspond to the file systems of those servers. If you have the necessary permissions, in a Global Shell session you can access multiple servers from a single virtual file system, the OGFS.

The following command navigates to file system of the `abc.opsware.com` server:

```
$ cd /opsw/Server/@/abc.opsware.com/files
```

The next `ls` command displays OGFS subdirectories that correspond to native users of the managed server. Your security administrator specified these users with the `-l` option of the `aaa` command. These are not Opware users.

```
$ ls
Administrator LocalSystem
```

Native users might have different views of the managed server's file system.

Therefore, under each user, the OGFS presents different file systems for each user.

The following `cd` command drills down to the `Program Files` directory as seen by the `Administrator` user on the Windows server.

```
$ cd "Administrator/C/Program Files"
$ pwd
/opsw/Server/@/abc.opsware.com/files/Administrator/C/Program
Files
```

Next, list the files in the `Program Files` directory:

```
$ ls -l
Accessories
Common Files
ComPlus Applications
Internet Explorer
Messenger
. . .
```

Although these files reside in a directory on the managed server's file system, you are in the OGFS, as shown by the preceding `pwd` command. To verify that you are in a Global Shell session (and not in a session running on the managed server), enter the following commands:

```
$ whoami jdoe
$ uname -a
Linux m171.dev.opsware.com 2.4.21-32.ELsmp #1 SMP Fri Apr 15
21:17:59 EDT 2005 i686 GNU/Linux
```

- 7** Copy a file from the OGFS to a managed server.

By entering the `cd` command, go to your home directory in the OGFS, for example:

```
$ cd
$ pwd
/home/jdoe
```

Next, create a simple text file in your home directory:

```
$ echo "this is text" > myfile.txt
$ cat myfile.txt
this is text
```

Copy the file that you just created to a directory in the file system of a managed server. The following command copies `myfile.txt` to the `C:\temp` directory of the `abc.opsware.com` server:

```
$ cp myfile.txt \
/opsw/Server/@/abc.opsware.com\
/files/Administrator/C/temp/afile.txt
```

Do not copy large files between the OGFS and managed servers. Copy only small files, such as configuration files.

- 8** Log on to a managed server with `rosh`.

In the preceding steps, you accessed the file system of a managed server from within a Global Shell session. In this step, from the Global Shell you log on to a managed server with `rosh`. After you log in, you interact with the command-line environment (MSDOS or Unix shell) of the managed server.

The following `rosh` command logs in as Administrator to a Windows managed server named `abc.opsware.com`:

```
$ cd /opsw/Server/@/abc.opsware.com
$ rosh -l Administrator
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

The prompt indicates that you are now in the command-line environment of the managed server. Enter the `ipconfig` and `hostname` commands:

```
C:\WINNT\system32>ipconfig
ipconfig
```

```
Windows 2000 IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```

Connection-specific DNS Suffix . : opsware.com
IP Address. . . . . : 192.168.8.217
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 192.168.8.1
```

```
C:\WINNT\system32>hostname
hostname
abc
```

Terminate the remote login with the `exit` command:

```
C:\WINNT\system32>exit
```

Enter the `uname` command to verify that you have returned to the Global Shell session:

```
$ uname -a
Linux m171.dev.opsware.com 2.4.21-32.ELsmp #1 SMP Fri Apr 15
21:17:59 EDT 2005 i686 GNU/Linux
```

9 Create a script that runs across servers.

A Global Shell script can iterate within the OGFS and run the `rosh` command to execute native commands on multiple servers. The example script shown in this step iterates through the servers of the public device group named All Windows Servers. On each server, the script runs the `ipconfig` command with the `rosh` command. In this example, substitute your Opware user name for `jdoe`.

First, return to your home directory in the OGFS:

```
$ cd
$ cd public/bin
$ pwd
/home/jdoe/public/bin
```

Next, run the `vi` editor:

```
$ vi
```

In `vi`, insert the following lines to create a bash script:

```
#!/bin/bash
# This is simple_iterate.sh.
```



```
# Change jdoe to your user name.

OUTFILE="/home/jdoe/public/bin/ipconfig_all.txt"
rm -f $OUTFILE

cd "/opsw/Group/Public/All Windows Servers/@/Server"

for SERVER_NAME in *
do
    echo ---- $SERVER_NAME
    echo ---- $SERVER_NAME >> $OUTFILE
    rosh -n $SERVER_NAME -l Administrator \
        "ipconfig" >> $OUTFILE
done
# Last line in simple_iterate.sh.
```

Save the file in vi, naming it `simple_iterate.sh`. Quit vi.

Change the permissions of `simple_iterate.sh` with `chmod`, and then run it:

```
$ chmod 755 simple_iterate.sh
$ ./simple_iterate.sh
---- abc.opsware.com
---- gist.opsware.com
---- hare.opsware.com
---- m33.opsware.com
. . .
```

As the script runs, it echos the name of each server to `stdout`, and redirects the output of the `ipconfig` command to the `ipconfig_all.txt` file. Enter the `more` command to view the contents of `ipconfig_all.txt`:

```
$ more ipconfig_all.txt
---- abc.opsware.com
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection: . . .
```

10 Learn more.

Here are a few suggested tasks for learning more about the OGFS and the Global Shell:

- Explore the folders and contents under `/opsw/Library`, comparing them with the Library windows of the SAS Client.
- If you have Opsware NAS installed, navigate to the `/opsw/Net*` (network) directories. For descriptions of these directories, see “Network Directories” on page 577.
- On Windows servers, examine the `registry` and `complus` directories under

```
/opsw/Server/@/server-name.
```

- List the files in the `method` directory, also under `/opsw/Server/@/server-name`. These files are the executables of the Opware Command-Line Interface (OCLI), which enables you to perform Opware SAS functions from within the Global Shell. To learn how to run the CLI methods, see the *Opware® Automation Platform Developer's Guide*.

Global Shell Examples

The examples in this section use `bash`, the default shell of a Global Shell session. These are relatively simple examples. For more complex examples, including those with method invocations and search filters, see the *Opware® Automation Platform Developer's Guide*.

Opening a Global Shell Session

You can open a Global Shell session with an `ssh` client or from within the SAS Client. When you open a session, the working directory is `/home/user-name`.

To open a Global Shell session with an `ssh` client, perform the following steps:

- 1** On a host that is not an Opware core server or a managed server, open a terminal window.
- 2** In the terminal window, enter an `ssh` command with the following syntax:

```
ssh -p 2222 user-name@ogfs-host
```

To use this command, port 2222 must be open on the firewall that protects the OGFS server. The `user-name` is your Opware user (login) and the `ogfs-host` is the host name (or IP address) of the core server running the OGFS. The Opware user name is not case sensitive. After you enter the `ssh` command, the OGFS prompts for the password of the Opware user.

To open a Global Shell session from within the SAS Client, from the **Actions** menu, select **Global Shell**.

Finding Servers in the OGFS

List the names of all servers that you can manage with Opware SAS:

```
ls /opsw/Server/@
```

List the IDs of the servers:

```
ls -a /opsw/.Server.ID
```

Find all servers in the `.opsware.com` domain by specifying the wildcard character (*):

```
ls -d /opsw/Server/@/*.opsware.com
```

List all servers in the Atlanta facility:

```
ls /opsw/Server/@Facility/Atlanta/@
```

List the servers in the public device group named Alpha:

```
ls /opsw/Group/Public/Alpha/@/Server
```

List the servers in the All Windows Servers group, first with backslashes to escape the spaces in the group name, then by enclosing the option in single quotes:

```
ls /opsw/Group/Public/All\ Windows\ Servers/@/Server
ls '/opsw/Group/Public/All Windows Servers/@/Server'
```

List the servers of the Widget customer:

```
ls /opsw/Customer/Widget/@/Server
```

The following two commands display the same output, the servers in the Atlanta facility that belong to the Green customer:

```
ls /opsw/Server/@Facility/Atlanta/@Customer/Green/@
ls /opsw/Server/@Customer/Green/@Facility/Atlanta/@
```

Getting Server Information from the OGFS

List the Opsware ID and of the server named `m256.opsware.com`:

```
cd /opsw/Server/@/m256.opsware.com
cat self:i ; echo
```

(The preceding `echo` command is optional. It generates a new line character, which makes the output easier to read. The semicolon separates `bash` statements entered on the same line.)

List the name of the server with an Opsware ID of `340039`:

```
cat /opsw/.Server.ID/340039/self
```

By iterating through the server names with a `for` loop in `bash`, display the platform (operating system) name for each server:

```
cd /opsw/Server/@
for SERVER_NAME in *
do
    cat $SERVER_NAME/attr/platform
done
```

Display the amount of RAM in the server named `abc.opsware.com`:

```
cd /opsw/Server/@/abc.opsware.com
grep Quantity Memory/RAM/info
```

Display the network interfaces of a the server named `blizzard.opsware.com`:

```
cd /opsw/Server/@/glengarriff.snvl.dev.opsware.com/Interface
for INTERFACE_NAME in *
do
    echo ..... $INTERFACE_NAME .....
    grep Interface "$INTERFACE_NAME/info"
    echo ""
done
```

Browsing a Server's File System or Registry

List all of the files the `C:\ Program Files` directory of the Windows server named `abc.opsware.com`:

```
cd /opsw/Server/@/abc.opsware.com/files/Administrator
ls C/Program\ Files
```

List the registry keys of the `abc.opsware.com` server:

```
cd /opsw/Server/@/abc.opsware.com/registry/\ Administrator/
ls *
```

List the contents of the `/var` directory on the Unix server named `m256.opsware.com`:

```
/opsw/Server/@/m256.opsware.com/files/root
ls var
```

Managing Custom Attributes

On the server `abc.opsware.com`, create a custom attribute named `MyGreeting` with the value `hello there`:

```
cd /opsw/Server/@/abc.opsware.com/CustAttr
echo -n "hello there" > MyGreeting
cat MyGreeting
```

Execute `runit.bat` on the `abc.opsware.com` server, passing the value of the `MyTest` custom attribute as a command-line parameter for `runit.bat`:

```
cd /opsw/Server/@/abc.opsware.com
TESTPARAM=`cat CustAttr/"My Test"`
rosh -l Administrator "C:\temp\runit.bat $TESTPARAM"
```

- When you create or edit custom attributes within the OGFS, Opware SAS preserves leading and trailing whitespace characters in custom attribute values.

Copying Files Within the OGFS

Do not use the techniques in this section to copy large files. The OGFS is not designed distribute large amounts of data. However, you can use these techniques for copying small files (such as configuration files) to and from managed servers.

Copy `myfile.txt` from the home directory in the OGFS of the `jdoue` user to the `C:\temp` directory of the Windows server named `abc.opsware.com`:

```
cp /home/jdoe/myfile.txt \
  /opsw/Server/@/abc.opsware.com/files/Administrator/C/temp
```

Copy `myfile.txt` from the home directory in the OGFS of the `jdoue` user to the `/tmp` directory of the Unix server named `m25.opsware.com`:

```
cp /home/jdoe/myfile.txt \
  /opsw/Server/@/m256.opsware.com/files/root/tmp
```

Copy the `C:\temp\myfile.txt` file from the `abc.opsware.com` server to the `m344.opsware.com` server:

```
cp /opsw/Server/@/abc.opsware.com/files/\
  Administrator/C/temp/myfile.txt \
  /opsw/Server/@/m344.opsware.com/files/\
  Administrator/C/temp/myfile.txt
```

Copying Files Between the OGFS and a Development Server

You can securely copy files between the OGFS and a server that is not part of Opsware SAS. To copy the files, perform the following steps:

- 1** On a host that is not an Opsware core server or a managed server, open a terminal window.
- 2** In the terminal window, enter either the `scp`, `sftp`, or `rsync` command and specify port 2222, your Opsware user name, and the host running the OGFS.

The following three `scp` examples perform the same operation: They copy the file `myscript.sh` from the local machine to the file `/home/jdoe/myscript.sh` in the OGFS. The Opsware user is `jdoue` and the host running the OGFS is `192.168.166.178`.

```
scp -P 2222 myscript.sh jdoe@192.168.166.178:myscript.sh
scp -P 2222 myscript.sh jdoe@192.168.166.178:/home/jdoe
scp -P 2222 myscript.sh jdoe@192.168.166.178:
```

The following example copies `myscript.sh` from the home directory of `jdoe` in the OGFS to the local machine:

```
scp -P 2222 jdoe@192.168.166.178:myscript.sh myscript.sh
```

The following `sftp` example copies `myscript.sh` from the local machine to the OGFS:

```
sftp -oPort=2222 jdoe@192.168.166.178
Connecting to 192.168.166.178...
```

```
Opware Global Shell
```

```
jdoe@opsware's password:
sftp> put myscript.sh
. . . .
```

The following `rsync` example transfers files from `/path` on the local machine to `/other/path` in the OGFS:

```
rsync -av -e "ssh -p 2222" /path \
jdoe@192.168.166.178:/other/path
```

Logging on to a Managed Server With `rosh`

The next three `rosh` commands perform the same operation: logging on to the Windows server named `abc.opsware.com` as the `Administrator` user. After logging on, the current working directory on the remote shell is the default working directory of the `Administrator` Windows user. These `rosh` commands require different options, depending on the current working directory in the OGFS. For example, the first `rosh` command does not require the `-n` (server name) and `-l` (user) options because the option values can be inferred from the current working directory of OGFS. The options of the following three `rosh` commands differ because of the current working directory:

```
cd /opsw/Server/@/abc.opsware.com/files/Administrator
rosh
. . .
exit
. . .
cd /opsw/Server/@/abc.opsware.com
rosh -l Administrator
...
exit
. . .
cd /home/jdoe
rosh -n abc.opsware.com -l Administrator
...
exit
```

The next `rosh` command logs into the Unix server named `m256.opsware.com` as the `root` user with the current working directory of `/tmp`:

```
rosh -n m256.opsware.com -l root -d /tmp
```

Running OGFS Scripts on Managed Servers With `rosh`

The next sequence of commands create a `.BAT` script in the OGFS and then run the script on a Windows managed server. Created with `echo` statements, the `myfile.bat` script resides in the OGFS under `/home/jdoe/public/bin`. (Note that `myfile.bat` does not reside in the file system of the managed server.) The `myfile.bat` script contains three commands: `ipconfig`, `cd`, and `dir`. The `rosh` command runs `myfile.bat` on the server named `abc.opsware.com` as the Administrator Windows user. The following commands create a local `.BAT` script and run it remotely with `rosh`:

```
cd /home/jdoe/public/bin

echo ipconfig > myfile.bat
echo "cd c:\temp" >> myfile.bat
echo dir >> myfile.bat

rosh -n abc.opsware.com -l Administrator -s ./myfile.bat
```

Create a script named `who.sh` in the `/home/jdoe/public/bin` directory of the OGFS and then run `who.sh` on the server named `m256.opsware.com`:

```
cd /home/jdoe/public/bin

echo \#\!\bin\sh > who.sh
echo "uname -n" >> who.sh
echo id >> who.sh
echo pwd >> who.sh

rosh -n m256.opsware.com -l root -s ./who.sh
```

Running Native Programs on Managed Servers With `rosh`

The next two `rosh` commands run the `dir` and `ipconfig` MSDOS commands on the Windows server named `abc.opsware.com`. Note that the native MSDOS commands are enclosed in quotes. Because the server name and user (login) can be inferred from the current working directory, the first `rosh` command omits the `-n` and `-l` options, as shown in the following code:

```
cd /opsw/Server/@/abc.opsware.com/files/Administrator
rosh "dir & ipconfig"
. . .
```

```
cd /home/jdoe
rosh -n abc.opsware.com -l Administrator "dir & ipconfig"
```

Run the `ipconfig` command on `abc.opsware.com` and redirect the output to a file in home directory of `jdoe` in the OGFS:

```
rosh -n abc.opsware.com -l Administrator "ipconfig" \  
> /home/jdoe/ipconfig_ouptput.txt
```

On the Unix server named `m256.opsware.com`, run the `uname` and `ls` commands as root:

```
rosh -n m256.opsware.com -l root "uname -a; ls /tmp"
```

Within a `for` loop in `bash`, run the MSDOS `ipconfig` command on each server in the All Windows device group:

```
cd /opsw/Group/Public/All\ Windows\ Servers/@/Server

for SERVER_NAME in *
do
    echo ..... $SERVER_NAME .....
    rosh -n $SERVER_NAME -l Administrator "ipconfig"
    echo ""
done
```

Character Encoding for the OGFS

To support international environments, the OGFS can display information in different character encodings such as Shift-JIS (Japanese) and EUC-KR (Korean). You can control the encoding of Global Sessions in the following ways:

- To specify the encoding of your Global Shell sessions, in the Terminal and Shell Preferences of the SAS Client, select an item from the Encoding drop-down list.
- To change the encoding of an active Global Shell session, run the `swenc` command with the `-e` option.

If you change the encoding of an active session, you must also change the encoding of the terminal application for that session. This procedure varies according to the terminal application.

Terminal Application Configuration

The terminal application that is hosting a Global Shell or Remote Terminal session must be configured to use the same encoding expected by the session. If the encodings do not match, the data might be displayed incorrectly.

When the SAS Client launches the terminal application, it composes the command specified by the Terminal Client field in the Terminal and Shell Preferences. If the Terminal Client field includes the %e substitution variable, the SAS Client replaces %e with an encoding name. For Global Shell sessions, this encoding name is specified by the Encoding field of the Terminal and Shell Preferences. For Remote Terminal sessions, this encoding name is the value of the Encoding field in the Properties section of the Server Explorer. If the terminal application does not support the encoding that replaces the %e variable, or if the %e variable is not specified, you must change the encoding manually in the terminal application after it starts.

Data that Cannot Be Displayed

Data that cannot be displayed might be from a managed server (such as the contents of files) or it might be the name of an object in the Opware model. If the session's encoding does not support the data to be displayed, the data often appears as question marks. (However, it might appear as other characters such as exclamation points.) The session attempts to display this data with the current encoding. Usually, this data cannot be accessed. To access this data, select a compatible encoding for the session.

Objects in the Opware model, such as Facility and Server, appear as file names in the OGFS. If these file names contain characters that cannot be represented by the encoding of the session, they are displayed as question marks, appended by the Opware ID of the object. In the following example, the IDs are 10002 and 11002:

```
New York
Paris
Montr?al~10002
??~11002
```

If the model object does not have an ID, such as a custom attribute, then the session attempts to display the name with the current encoding.

LANG and LC_CTYPE Environment Variables

Many Unix commands (such as `ls`) rely on the character encoding, which is determined by the `LANG` or `LC_CTYPE` environment variables. In a Global Session, if the encoding is changed with the `swenc` command, the system attempts to reset these variables.

Opware SAS determines the new value of the `LANG` variable with the following process:

- 1** The value of `LANG` is generated by combining the language of the user's profile in the SAS Web Client with the current session encoding. For example, if the language is English and the session encoding is UTF-8, `LANG` is set to `en_US.utf8`.
- 2** The value determined by the preceding step is compared with the set of valid locales on the OGFS server (according to the output of `locale -a`). If the value is a valid locale, `LANG` is set to this value.
- 3** If the value is not a valid locale, the system attempts to find a valid locale that specifies the user's language without the encoding. For example, if the user's language is English and the session encoding is EUC-JP, and this combination does not form a valid locale, `LANG` is set to `en_US`. If no matching locale is found, `LANG` is left unspecified.

The new value of the `LC_CTYPE` variable is determined in the following order:

- 1** Opware SAS attempts to find a valid locale that matches the session encoding, regardless of the language.
- 2** If a valid locale is found, `LC_CTYPE` is set to this locale. For example, if the session encoding is EUC-JP, the `LC_CTYPE` variable is set to `ja_JP.eucjp`.
- 3** If no matching locale is found, `LC_CTYPE` is left unspecified.
- 4** If Opware SAS cannot set the `LANG` or `LC_CTYPE` variables with the preceding process, you should set them manually.

Transcoded Data in a Managed Server

Transcoding is the conversion of data from one character encoding to another. Opware SAS automatically transcodes some of the data between Global Shell sessions and other sources of data. For example, the file names of managed servers are transcoded, but the

contents of the files are not. To see which data is transcoded, see Table 10-1. To display the transcoding mode of the current Global Shell session, enter the `swenc` command with no options.

Table 10-1: Data Transcoded for Global Shell Sessions

DATA	TRANSCODING
Objects in the Opsware model space, such as <code>Facility</code> , <code>Customer</code> , and <code>Server</code> . These objects are stored in the Opsware Model Repository (database) in UTF-8.	Between UTF-8 and the session encoding.
File and directory names of managed servers.	Between the managed server encoding and the session encoding.
Meta-data of managed servers, such as user names and registry key names.	Between the managed server encoding and the session encoding.
File contents of managed servers.	None
Contents of Windows registries, services, COM objects, and IIS metabases.	None
<code>rosh</code> : Contents of saved scripts executed on managed servers (a <code>rosh push</code> operation).	None
<code>rosh</code> : Ad-hoc scripts executed on managed servers.	None
<code>rosh</code> : Command-line arguments to programs executed on managed servers.	None
<code>rosh</code> : Data streams (such as <code>stdin</code> and <code>stdout</code>) of programs executed on managed servers.	None
<code>rosh</code> : Data streams of <code>rosh jump</code> operations.	None
OGFS <code>home</code> , <code>tmp</code> , and <code>var/tmp</code> directories.	None

Disabling the Transcoding of Managed Server Data

On Unix servers, file and directory names can contain characters in arbitrary encodings. When accessed through the OGFS, file and directory names are transcoded by Opware SAS. If the encoding of the names does not match the default encoding of the managed server, the transcoded data might be unusable.

You can disable transcoding with the `swenc` command. To turn transcoding on or off, use the `-T` option:

```
swenc -T {on | off}
```

If transcoding is disabled, file and directory names are passed unmodified from the managed servers. Therefore, you must manually configure the encoding of the terminal application to display the names correctly.

Windows servers store their file system data internally in the UTF-16 encoding. Because the encoding is known, transcoding is performed correctly and does not need to be disabled. Therefore, the `-T` option of the `swenc` command has no effect on Windows servers. For more information, see “swenc Syntax” on page 562.

Global Shell Error Messages

The Global Shell feature provides the file system error messages that are described in Table 10-2

Table 10-2: Global Shell Errors

ERROR	DESCRIPTION	ACTION
Input/output error	Your session has exceeded the time-out limit or the Agent is not running.	Start a new session or check the status of the Agent.
Operation not permitted.	No password was found.	Verify that you have a valid password.
Permission denied.	You are not allowed to view a directory. This does not mean that the directory does not exist on a given server. See the <i>Opware® SAS Administration Guide</i> for more information.	Verify that you have <code>readFileSystem</code> permissions.

Table 10-2: Global Shell Errors

ERROR	DESCRIPTION	ACTION
RFS Specific error	You do not have permissions on the managed server. For example, this error will occur if you are trying to perform an operation on a managed server and you do not belong to the Administrators group that has the required permissions assigned to it.	You must have a set of permissions to perform operations on managed servers. To obtain these permissions, contact your Opware administrator. See the <i>Opware® SAS Administration Guide</i> for more information.

Remote Terminal

With Opware SAS, you can log on to a managed server in a terminal window in two ways:

- The Remote Terminal feature, as described in this section.
- The `rssh` command, entered in a Global Shell session.

The Remote Terminal feature opens a terminal window for Unix servers or an RDP client window for Windows servers. Unlike a Global Shell session, a Remote Terminal session does not provide access to the OGFS.

You can specify your terminal and RDP client preferences for Remote Terminal and Global Shell sessions in the Set Preferences window. See “Terminal and Shell” on page 92 in Chapter 3 for more information.

Prerequisite for a Remote Terminal

This feature requires Opware login permissions on the managed server. See the *Opware® SAS Administration Guide* for more information. You cannot log into a remote terminal with a user name or password that contains multi-byte characters.

In order to open a Remote Terminal session on a Windows managed server running Windows Firewall, you must set an exception that is not enabled by default. On the managed server, run Windows Security Center, then select Windows Firewall ► Exceptions ► Remote Desktop.

This feature must be able to establish a loopback connection on the machine running the SAS Client. Some firewall and VPN utilities have settings that prevent loopback connections.

Opening a Remote Terminal

In the Server Explorer of the SAS Client, perform the following steps:

- 1** Select a managed server.
- 2** Open the managed server.
- 3** From the **Actions** menu, select **Remote Terminal**.

Chapter 11: Distributed Script Execution

IN THIS CHAPTER

This section discusses the following topics:

- Distributed Script Execution
- Ways to Initiate Script Operations
- Script Management Tasks
- Script Execution
- Script Execution Results
- Error Resolution for Script Execution
- Opware SAS Custom Extensions

Distributed Script Execution

This section provides information about the Distributed Script Execution feature within Opware SAS and contains the following topics:

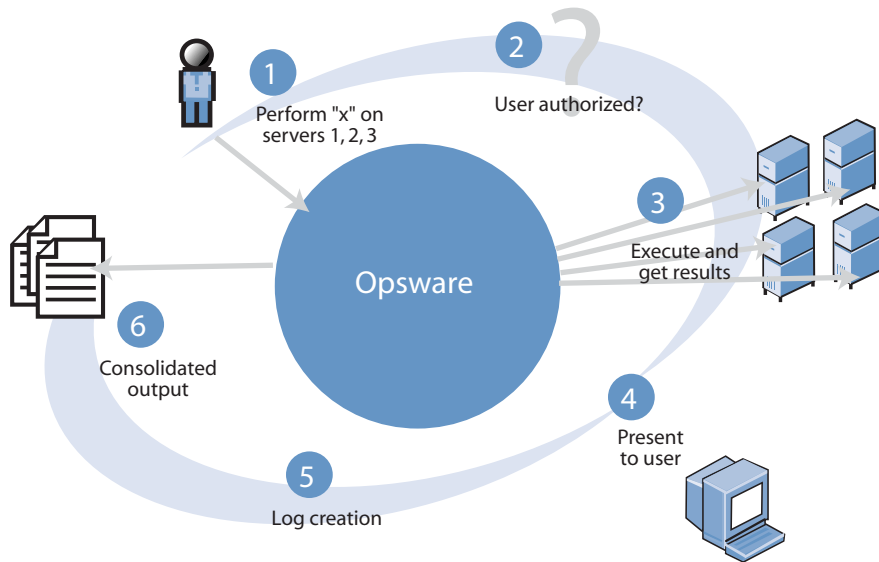
- Overview of Distributed Script Execution
- Scripts Types – My Scripts, Shared Scripts, and Ad-Hoc Scripts
- Script Execution Functionality
- Run Distributed Script Link

Overview of Distributed Script Execution

The Script Execution feature provides tools for automating the management and execution of server scripts. Previously, a user created a script and then manually executed the script on individual servers, one server after another. With the Script Execution feature, a user performs all script tasks from one location – the SAS Web Client.

From the SAS Web Client, you can create or upload a script, set it up to run simultaneously across multiple Unix or Windows servers, and monitor it as it executes on each server. After a script runs, job- and server-specific execution results are available for review. You can modify, delete, or rerun the script again at a later date. See Figure 11-1

Figure 11-1: Script Execution Process



You need a specific set of feature permissions to manage and execute scripts. You'll also need permissions to access the servers associated with customers, facilities, or server groups. To obtain these permissions, contact your Opsware administrator. For more information, see the Permissions Reference Appendix in the *Opsware® SAS Administration Guide*.

Scripts Types – My Scripts, Shared Scripts, and Ad-Hoc Scripts

The Script Execution Subsystem supports the three major types of scripts for Unix and Windows operating systems: Unix/Linux shell, Windows batch (.BAT), and Windows Visual Basic (VBScript).

After you create or upload Unix or Windows scripts in Opsware SAS, the scripts are stored in Opsware SAS in one of two ways:

- As private scripts, accessible only to the user who created them. In Opsware SAS, private scripts are called My Scripts.

My Scripts can only be edited, deleted, or executed by the user who created the script. My Scripts are intended for personal use.

- As public scripts, accessible to all Script Execution users. In Opsware SAS, public scripts are called Shared Scripts.

A third type of Opsware SAS script is created (or uploaded) and then immediately executed by a user. The script is intended for one-time use and is not stored in Opsware SAS. In Opsware SAS, this type of script is referred to as an Ad-Hoc Script. During the Ad-Hoc Script creation and execution process, only one user has access to the script.

After you create a script and store it as a specific type of script in Opsware SAS, you cannot convert the script to the other type of script. My Scripts cannot be converted to Shared Scripts (and vice versa).

Script Execution Functionality

The Script Execution feature provides three basic functions:

- Script management
- Script execution
- Viewing script execution results

Script Management Tasks

Script Management tasks include:

- Viewing contents of stored My Scripts or Shared Scripts
- Creating (or uploading) My Scripts or Shared Scripts for storage in Opsware SAS
- Editing or deleting stored My Scripts or Shared Scripts
- Viewing version history of stored My Scripts or Shared Scripts

Script management functionality is handled by two Opsware SAS components – the Command Engine and the SAS Web Client. The Command Engine handles the entry of scripts into the Opsware Model Repository (the script storage location in Opsware SAS) and the versioning of stored scripts. The SAS Web Client provides the user interface for

script management activities. It provides tools that allow users to create or upload scripts for storage. It also allows users to create Ad-Hoc (one-time-use, not stored) scripts for immediate execution.

Script Execution Tasks

Script execution tasks include:

- Executing a My Script or Shared Script, stored in Opware SAS, on one or more servers
- Creating (or uploading) an Ad-Hoc Script and then immediately executing it on one or more servers

Script Execution Functionality

Script execution functionality is handled by three Opware SAS components – the SAS Web Client, the Command Engine, and the Opware Agent. The SAS Web Client provides the user interface for script execution activities. Script execution tasks are automated by a wizard that leads users through the following script execution steps:

- 1** Select scripts.
- 2** Select servers.
- 3** Specify execution options.
- 4** Confirm settings.
- 5** Execute scripts across one or more servers.

During script execution on the servers, the Command Engine runs a script that issues an execution command to the Opware Agent on each server. Each Opware Agent handles script execution and sends execution results to the Command Engine.



Execution of a script on the managed servers cannot be rolled back.

Script Execution Results Functionality

Execution results display immediately after a script runs and can be viewed any time after a script is executed. The functionality that displays execution results is handled by two Opware SAS components – the Command Engine and the SAS Web Client. The Command Engine enters the execution results data into the Model Repository. The SAS

Web Client retrieves and displays execution results data from the Model Repository and provides tools for the user to download execution results data (output and error files) as a zip file.

Ways to Initiate Script Operations

In the SAS Web Client, you can initiate a Script Execution operation in the following three ways:

- Scripts link
- Run Distributed Script link
- By selecting **Server ► Run Script** from these initiating scripts from the Scripts link and from the Run Distributed Script Wizard on the Home page.

Scripts Link

The Scripts link displays tools for managing scripts. Select this link to create or upload scripts that you want to save or run, and to view, edit, or delete scripts that have already been stored in Opware SAS. The Scripts link is located on the navigation panel under Software. See Figure 11-2.

Figure 11-2: The Scripts Link Is Used to Create, Run, Upload, Edit, Delete, or View Scripts



Run Distributed Script Link

The quickest way to execute a script that is stored in Opware SAS, or to create and immediately execute an Ad-Hoc Script, is to select the Run Distributed Script link in the Tasks panel of the SAS Web Client. See Figure 11-3.

Figure 11-3: Click the Run Distributed Scripts Link to Launch the Script Execution Wizard

Tasks		
OS Provisioning	Software Provisioning	Power Tools
Prepare OS	Deploy Code	Launch Opware SAS Client Run Distributed Script Run Custom Extensions

You can view the status of scripts in the My Jobs area of the SAS Web Client Home page, which displays information about jobs that have run, are currently running, or are scheduled to run, including script execution jobs. Through My Jobs, you can display script execution results. The name of the job is also a hyperlink to a pop-up window that allows you to change scheduling information for that job. In addition to the name, start time, and status, the number of servers affected by the job also appears.

The hyperlink to script execution jobs is called Run Script. A particular execution event can be identified by the start time of the execution event. Click any Run Script name to view the results of that particular script execution if it has completed. Otherwise, information about when the job is scheduled to run appears instead.

You can display a complete list of My Jobs by clicking the See All link in the My Jobs area of the home page, or by clicking the My Jobs link from the navigation panel.

Script Management Tasks

Supported script management tasks include:

- Script Creation Guidelines
- Viewing the Scripts List
- Editing, Deleting, and Downloading a Script
- Script Version History

Script Creation Guidelines

Opware SAS supports the three major types of scripts for Unix and Windows operating systems: Unix/Linux shell, Windows batch (.BAT), and Windows Visual Basic (VBScript).

When creating scripts, adhere to the following guidelines:

- 4 MB is the maximum size allowable for a script.
- When you create a Unix shell script with a language other than the Bourne (sh) shell, use the sh-bang (!) format at the top of the script to specify the correct command interpreter. The command interpreter needs to be present on the Opware-managed server.

For example, if you are using Perl, the beginning of the script would contain the following line:

```
#!/usr/bin/perl
```

The following example shows a short Perl script (it displays “hello world”):

```
#!/usr/bin/perl
print "hello world\n"
```

- VBScripts are executed by the VBScript interpreter on the Windows server.
- To access command line parameters with Unix shell commands, use the following convention: \$1 \$2 . . .
- To access command line parameters with Windows .BAT, use: %1 %2 . . .
- Script lines do not need to be terminated in a specific way. But with Windows scripts, Opware SAS converts all \n to \r\n. With Unix scripts, all \r\n are converted to \n.
- Scripts should be written to send error output to standard error (file descriptor #2).
- Scripts should use the standard convention of returning a zero code to indicate success. For other return codes, there is no standard code system to follow. Create unique non-zero return codes to handle each type of error.

Creating or Uploading a Script

You can create scripts in the SAS Web Client or by uploading a script into Opware SAS. To create or upload a My Script or a Shared Script, perform the following steps:

- 1** From the navigation panel, select Software ► Scripts.
- 2** The Scripts page has two tabs: My Scripts and Shared Scripts.

- To create or upload My Scripts, select the My Scripts tab, and then New Script. The New Script page appears.
- To create or upload a Shared Script, select the Shared Scripts tab, and then New Script. The New Script page appears, as Figure 11-4 shows.

Figure 11-4: Scripts: New Script Page

Scripts: New Script

[Return to Scripts](#)

Properties

Name:	<input type="text"/>
Type:	<input type="text" value="Unix Shell"/>
Shared:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Changes Server?	<input type="radio"/> No <input checked="" type="radio"/> Yes

Script Contents

Enter Script Contents:

Upload Script:

Encoding of script

Local Path to Script:

Usage Notes

Usage Notes are required

- 3** On the Scripts: New Script page, enter the following data under Properties:
 - Enter the name of the script. The name must be a unique shared-use or personal-use name.
 - Select the script type: Unix shell, Windows .BAT, or Windows VBScript.
 - If you are creating a Shared Script, select Yes next to Shared. If you are creating a My Script, select No.
 - In the Changes Server field, select No if the script does not modify the server, and Yes if it does. If you select Yes, locked servers cannot be selected to run that script.
- 4** Under Script Contents, enter or upload a script by performing one of the following tasks:
 - To upload a script, click **Upload Script**. In the Local Path to Script box, either manually enter the path to the script, or click **Browse** to locate the script.



When you upload a script, you must select the character encoding of the script's contents from the list. (Before storing the script, Opsware SAS converts the script contents from the encoding that you select to the UTF-8 encoding.)

- To create a script, click **Enter Script Contents** and manually enter the script in the text box.



The script editor does not recognize tabs and its functionality is browser-dependent.

- 5** In the Usage Notes section of the page, enter script details or other descriptive information.
- 6** Click **Save** to store the script. The script is saved in the Model Repository.

The Scripts page appears and confirms that the script is now stored. The script is included in the list of available Shared Scripts or My Scripts.

Viewing the Scripts List

After you save a script in Opware SAS, you can view it on the list of stored My Scripts or Shared Scripts. My Scripts can be viewed only by the user who created them, while Shared Scripts can be viewed by all users.

To view the list of stored My Scripts or Shared Scripts, perform the following steps:

- 1** From the navigation panel, select Software ► Scripts.
- 2** The Scripts page has two tabs: My Scripts and Shared Scripts.
 - To view the list of My Scripts, select the My Scripts tab.
 - To view the list of Shared Scripts, select the Shared Scripts tab.

A list of My Scripts or Shared Scripts displays. Each script name is also a link.

- 3** To view a script, click its name.

Editing, Deleting, and Downloading a Script

After you save a script in Opware SAS, you can edit, delete, or download the script. Before you edit or delete a script, you might want to view the script properties, contents, usage notes, and change log.



My Scripts are accessible only to the user who created them and can only be edited or deleted by this user.

Editing a Script

To edit a stored script, perform the following steps:

- 1** From the navigation panel, select Software ► Scripts.
- 2** The Scripts page has two tabs: My Scripts and Shared Scripts.
 - To locate a My Script, select the My Scripts tab.
 - To locate a Shared Script, select the Shared Scripts tab.

A list of scripts displays. Each script name is also a link.

- To view the script, click the name. The View Script page appears, displaying script properties, contents, and usage notes, as Figure 11-5 shows.

Figure 11-5: The View Script Page

Scripts: View Script | DiskSuite Break Mirror (Analyze/Test) ?

[Return to Scripts](#)

Properties		Run...	Download	Edit
Name:	DiskSuite Break Mirror (Analyze/Test)			
Type:	Unix Shell			
Shared:	Yes			

Script Contents		Edit
Changes Server?	Yes	
<pre>#!/bin/sh # exit upon error set -e # run first in test mode to make sure everything is kosher /opt/ISMbrkm/dsBreak.sh -t</pre>		

Usage Notes		Edit
<pre>Triggers the testing the separation of SDS mirrored root filesystems on a server using 'dsBreak.sh' (part of ISMbrkm). No changes to the server are made. The server's custom attributes are updated with the results of the test.</pre>		

- Click **Edit** in the Properties panel for details about script properties.
- On the Scripts: Edit Script page, Change Log information is now available. Select the Change Log tab to view the current script's version history.

- 6 Use the tabs on the Scripts: View Script page to edit script contents or the script name, and enter usage notes. See Figure 11-6.

Figure 11-6: View Scripts Page That Shows Properties, Contents, Usage Notes, and Change Log Tabs

Scripts: Edit Script | List /tmp Files Long Format

Return to [Scripts: View Script](#)

Properties	Contents	Usage Notes	Change Log
			1 Total
Contents Modified ▲		User	Comments
Wed Aug 27 15:26:18 2003		alfred	Initial upload View...

- To edit script contents, select the Contents tab. In the Edit Contents panel, select the Edit Script Contents radio button and edit the contents of the script.
 Instead of manually editing script contents, you can also upload new script contents. The uploaded script overwrites current script contents. To upload, select the Upload & Overwrite Script radio button and enter the location of the script you want to upload.
 After you edit script contents or upload new content, enter change log comments in the text box below the Edit Contents panel. Change log comments are required when you edit a script. When you are finished, click **Save**.
- To edit the name of the script, select the Properties tab. Edit the name that currently displays in the Name box and click **Save**.
- To enter usage notes, select the Usage Notes tab and enter information on the Edit Usage Notes panel. When finished, click **Save**.

Deleting a Script

To delete a stored script, perform the following steps:

- 1 From the navigation panel, select Software ► Scripts.
- 2 The Scripts page has two tabs: My Scripts and Shared Scripts.
 - To locate a My Script, select the My Scripts tab.
 - To locate a Shared Script, select the Shared Scripts tab.

A list of scripts displays. Each script name is also a link.

- 3 To review a script before you delete it, click the name. To return to the list of scripts, click the Scripts link in Return to Scripts (located at the top of the Scripts: View Script page).
- 4 On the Scripts page, select the scripts that you want to delete by clicking the box located to the left of the script name. You can delete more than one script at a time.
- 5 Click **Delete**.
- 6 The Delete Scripts confirmation window appears.
 - To review the list of scripts you selected for deletion, click **View Details**.
 - To cancel the entire operation, click **Cancel**.
 - To delete the selected scripts, click **Delete**.



After you delete a script, you can still view the results of executions performed with that script.

Downloading a Script

To download a stored script, perform the following steps:

- 1 From the navigation panel, select Software ► Scripts.
- 2 The Scripts page has two tabs: My Scripts and Shared Scripts.
 - To locate a My Script, select the My Scripts tab.
 - To locate a Shared Script, select the Shared Scripts tab.

A list of scripts displays. Each script name is also a link.

- 3 Click the name of the script to download.
- 4 On the Scripts page, click **Download**.
- 5 Select the character encoding of the target server from the list. Opware SAS converts the script contents from the UTF-8 encoding to the encoding that you select. Internally, Opware SAS stores the script in the UTF-8 encoding.
- 6 in the pop-up window for the encoding, click **Download**.

Script Version History

Version history for a script is maintained in a change log, which is stored with other My Script or Shared Script management information. Each time a script is modified, new script version information is created and stored.

Viewing Script Version History

To view script version history, perform the following steps:

- 1** From the navigation panel, select Software ► Scripts.
- 2** The Scripts page has two tabs: My Scripts and Shared Scripts.
 - To locate a My Script, select the My Scripts tab.
 - To locate a Shared Script, select the Shared Scripts tab.A list of scripts displays. Each script name is also a link.
- 3** To view the script, click the name. The Scripts: View Script page appears and displays script properties, content, and usage notes.
- 4** Click **Edit** in the Properties panel.
- 5** On the Scripts: Edit Script page, select the Change Log tab to access the change log and view version history for the current script.

The change log provides the following script version information:

- Date and time the script is modified
- Users who modified the script
- Comments associated with each script modification
- Script contents for that modification

Script Execution

This section provides information about script execution tasks, tips, and procedures and contains the following topics:

- Overview of Distributed Script Execution
- Script Execution Guidelines
- Executing My Script or Shared Scripts
- Creating and Executing an Ad-Hoc Script

Overview of Script Execution

A Script Execution Wizard automates script set up and execution processes and steps the user through the following execution stages (in the order shown):

- 1 Select Script:** You can select only one My Script or Shared Script for each execution run. You can select scripts in the Wizard or from the Scripts page by selecting Software ► Scripts in the navigation panel.
- 2 Select Servers:** You can select one or more servers or groups from the displayed list of available servers. Only servers running an operating system applicable to the selected script are shown (for example, only servers running Unix are shown for a Unix shell script).
- 3 Specify Options:** Runtime data, information, and execution options are entered at this stage.
- 4 Confirm Settings:** This stage allows the user to review settings prior to execution. Click **Next**.
- 5** On the Schedule and Notify page, you have the following options:
 - **Notify:** Choose the Condition option and set the parameters to send an email when the operation is completed. You can choose to have an email sent on any result, if the operation fails, or if the operation is successful. To add another email recipient, click the plus (+) button next to the Recipients field.
 - **Schedule:** Choose either **Run Now** to execute the operation immediately, or choose **Specify Time** to schedule the operation for a later time.

When you schedule a job for a server group, you can specify how the members of the group are determined. The membership of a dynamic server group changes based on the changes in your operational environment. If you have “Allow Run Refresh Jobs” permissions, you will see additional options. Select either of the following options:

- **Option 1:** Membership is determined based on the “Time of Confirm Selection.” Select this option to run the job on the servers that were in the group when you scheduled the job. Changes to the group membership do not affect the list of the servers that the job will run on.
- **Option 2:** Membership is updated when the job runs. Select this option to recalculate the group membership prior to running the job. Changes to group membership are reflected in the list of servers that the job will run on.



The time used for the scheduled job is specified in your preferred time zone which can be modified in My Profile. If you do not have the preferred time zone set, the time zone is derived from the Opware SAS core server (usually UTC).

6 Run Script: While the script executes, progress information displays about the total run and each server. When execution ends, summary information displays. After execution, script contents, output data, and error data can be immediately reviewed and downloaded.



The default amount of output data that Opware SAS stores is 10 KB. This amount can be modified by the Opware administrator.

Script Execution Guidelines

When executing a script, adhere to the following guidelines:

- No specific assumptions should be made about the execution environment. No particular environment variables are set.
- When executing processes on Unix servers, make sure long running processes (Web servers, databases, and so forth) are started as daemons. Also, make sure server processes properly daemonize themselves.
- For Windows servers, do not start anything that causes a window to open and wait for input.

Executing My Script or Shared Scripts

To execute My Script or Shared Scripts, perform the following steps:

- 1** Click the Run Distributed Script link in the Tasks area of the SAS Web Client home page to launch the Run Distributed Script Wizard.
- 2** On the Overview page, make sure that you select Saved Script.
- 3** Click **Start**.

Alternatively, you can initiate the script execution process by clicking Software ► Scripts on the navigation panel, and then selecting a script and clicking **Run**.

- 4** To list Shared Scripts, select the Shared Script tab. Or, to list My Scripts, select the My Scripts tab.

- 5** From the script list, locate the script and select the script's radio button located to the left of the script name.
- 6** Click **Next** to continue (or click **Previous** to return to the previous step).
- 7** At the Select Servers page, browse or search for a server or servers to use.
 - To browse, select the Browse tab to obtain a list of servers available to you. At the top of the page, use the Customers and Server Status to narrow your selection.
 - To search, select the Search tab. On the Search page, indicate search criteria by selecting the appropriate check box.

Only servers are listed that use the operating system appropriate for the type of script that you want to run. For information about a server, click the name of the server. To sort the server list by server name, IP address, OS version, facility, or customer, click the heading of the column that you want to sort. For example, to sort by customer, click the heading titled Customer.
- 8** From the server list, specify the servers that you want to use. Select one or more servers or groups for script execution.
- 9** Click **Next** to continue (or click **Previous** to return to the previous step).

- 10** On the Specify Options page, enter the runtime information, as Figure 11-7 shows.

Figure 11-7: The Specify Options Page

Specify Options

Specify the runtime user and command line parameters for the script.

Runtime User:

- Run as "root"
 Run As Specified User:

Username:

Password:

Confirm Password:

Script Output: Keep Discard

Only the last 10 KB of script output can be shown.

Script Timeout: minutes

How many minutes to wait before timing out script.

Command Line Parameters:

Usage Notes (Reference for Command Line parameters):

```
Print Working Directory
```

- Specify the runtime user. If you have the appropriate permission, you are able to execute the script as root or local system without entering a password. Otherwise, enter a user name and password for the servers you intend to execute on. The user name and password you use must be the same across all servers.
- Specify if you want to keep or discard script output. Only a portion of script output is saved (the amount of script output that is saved is configurable by the Opsware administrator, but the default is 10 KB).
- Enter a script time-out value in minutes.

This value is the amount of time a script has to complete execution activities on a server. If the script is not finished when the time-out value is reached, the script is stopped by Opsware SAS and a script error occurs.

Select a time-out value that is greater than the time required for execution to complete.

- Enter command line parameters.

Use the same syntax as when entering a script on a command line. For Unix scripts, use Bourne (sh) shell syntax. For Windows scripts, use `cmd.exe` parameter syntax.

- Add usage notes.

11 Click **Next** to continue (or click **Previous** to return to the previous step).

12 On the Confirm Settings page, review your script execution settings before you proceed. The Script to be run panel provides information about your script and the Servers panel displays the servers selected for script execution. The Confirm Settings page displays execution settings, as Figure 11-8 shows.

Figure 11-8: The Confirm Settings Page

Confirm Settings

Review the following script execution settings. Click 'Run Script' to run the script.

Script to be run:

Name: List /tmp Files Long Format
 Type: Unix Shell
 Run-Time User: root
 Command Line Parameters:
 Script Output: Keep
 Script Timeout: 2 minutes

Servers

	Name	IP Address	OS Version	Facility	Customer
<input checked="" type="checkbox"/>	dell test box	192.168.8.180	Linux 7.1	C06	Customer Independent

Cancel

< Previous

Run Script >

If you discover that script or server changes are needed, click **Previous** as many times as you need to return to the Script or Select Servers page.

13 On the Schedule and Notify page, you have the following options:

- **Notify:** Choose the Condition option and set the parameters to send an email when the operation is completed. You can choose to have an email sent on any result, if the operation fails, or if the operation is successful. To add another email recipient, click the plus (+) button next to the Recipients field.
- **Schedule:** Choose either **Run Now** to execute the operation immediately, or choose **Specify Time** to schedule the operation for a later time.

When you schedule a job for a server group, you can specify how the members of the group are determined. The membership of a dynamic server group changes based on the changes in your operational environment. If you have "Allow Run Refresh Jobs" permissions, you will see additional options. Select either of the following options:

- **Option 1:** Membership is determined based on the "Time of Confirm Selection." Select this option to run the job on the servers that were in the group when you scheduled the job. Changes to the group membership do not affect the list of the servers that the job will run on.
- **Option 2:** Membership is updated when the job runs. Select this option to recalculate the group membership prior to running the job. Changes to group membership are reflected in the list of servers that the job will run on.



The time used for the scheduled job is specified in your preferred time zone which can be modified in My Profile. If you do not have the preferred time zone set, the time zone is derived from the Opware SAS core server (usually UTC).

14 Click **Run Script** to execute the script. While the script executes, progress information displays about the total run and each server. When execution ends, summary information displays. After execution, script contents, output data, and error data can be immediately reviewed and downloaded.

If you select to run the job at that time, a progress bar appears that shows the progress of the script execution.

15 After script execution, summary details on each server and the total job display. An ID number at the top of the page identifies the job.

- To see script output, summary details and information about errors that might have occurred, click **View Details**.
- For each server, you can click **Download** to obtain a zip file (`results.zip`) that contains script execution output and error data.

The data is in two files called `stdout` (output data) and `stderr` (error data), in a directory named `<servername>`. For example, for a server named `m0043`, the output and error files would be located as follows: `m0043/stdout` (output file for server named `m0043`) and `m0043/stderr` (error file for server named `m0043`).

16 Click **Close** to exit the wizard.

Creating and Executing an Ad-Hoc Script

An Ad-Hoc script is written (or uploaded) and then executed without being stored in Opsware SAS.

Ad-Hoc script setup and execution are handled by the same wizard that steps the user through the processes used for stored scripts. However, the initial steps differ because Ad-Hoc script creation is integrated with execution activities.

Perform the following steps to create or upload an Ad-Hoc script, and then execute the script:

- 1** Click the Run Distributed Script link in the Tasks area of the SAS Web Client home page to launch the Run Distributed Script Wizard.

- 2 On the Overview page, click Define Ad-Hoc Script ► Start. The Define Script page appears, as Figure 11-9 shows.

Figure 11-9: The Define Script Page

Define Script

Specify the type and enter or upload the contents of the script you would like to run.

Type:

Script Contents:

Enter Script Contents:

Upload Scripts:

Local Path to Script:

- 3 Select the type of script that you are creating (Unix shell, Windows VBScript, or Windows .BAT).
- 4 For Script Contents, indicate if you are entering script contents or uploading the script:
 - To upload a script, click **Upload Script**. In the Local Path to Script box, either manually enter the path to the script or click **Browse** to locate the path.
 - To create a script, click **Enter Script Contents** and enter the script in the text box.



The Scripts editor does not recognize tabs and its functionality is browser-dependent.

- 5 Click **Next** to continue (or click **Previous** to return to the previous step).
- 6 On the Select Servers page, browse or search for the server or servers to use.

- To browse, select the Browse tab to obtain a listing of servers available to you. At the top of the page, use the Customers and Server Status filters to narrow your selection.
- To search, select the Search tab. At the Search page, indicate search criteria by selecting the appropriate check box.

Only servers are listed that use the operating system appropriate for the type of script that you want to run. For information about a server, click the name of the server.

7 From the list of servers, select one or more servers or groups for script execution.

8 Click **Next** to continue (or click **Previous** to return to the previous step).

9 On the Specify Options page, enter the following runtime information:

- Specify the runtime user. If you have the appropriate permission, you can execute the script as root or local system without entering a password. Otherwise, enter an appropriate user name and password.
- Specify if you want to keep or discard script output. Only a portion of script output is saved (the amount of saved script is configured by the Opsware administrator).
- Enter a script time-out value in minutes.

This is the amount of time a script has to complete execution activities on a server. If the script is not finished when the time-out value is reached, the script is stopped by Opsware SAS and a script error occurs.

Select a time-out value that is greater than the time required for execution to complete.

- Enter command line parameters.

Use the same syntax as when you enter a script on a command line. For Unix scripts, use Bourne (sh) shell syntax. For Windows scripts, use `cmd.exe` parameter syntax.

10 Click **Next** to continue (or click **Previous** to return to the previous step).

11 On the Confirm Settings page, review your script execution settings before you proceed to run the script. The Script to be run panel provides information about your script and the Servers panel displays the servers selected for script execution.

If you discover that script or server changes are needed, click **Previous** as many times as you need to return to the Script or Select Servers page.

12 On the Schedule and Notify page, you have the following options:

- **Notify:** Choose the Condition option and set the parameters to send an email when the operation is completed. You can choose to have an email sent on any result, if the operation fails, or if the operation is successful. To add another email recipient, click the plus (+) button next to the Recipients field.
- **Schedule:** Choose either **Run Now** to execute the operation immediately, or choose **Specify Time** to schedule the operation for a later time.

When you schedule a job for a server group, you can specify how the members of the group are determined. The membership of a dynamic server group changes based on the changes in your operational environment. If you have "Allow Run Refresh Jobs" permissions, you will see additional options. Select either of the following options:

- **Option 1:** Membership is determined based on the "Time of Confirm Selection." Select this option to run the job on the servers that were in the group when you scheduled the job. Changes to the group membership do not affect the list of the servers that the job will run on.
- **Option 2:** Membership is updated when the job runs. Select this option to recalculate the group membership prior to running the job. Changes to group membership are reflected in the list of servers that the job will run on.



The time used for the scheduled job is specified in your preferred time zone which can be modified in My Profile. If you do not have the preferred time zone set, the time zone is derived from the Opware SAS core server (usually UTC).

13 Click **Run Script** to execute the script. While the script executes, progress information displays about the total run and each server. When execution ends, summary information displays. After execution, script contents, output data, and error data can be immediately reviewed and downloaded.

If you select to run the job at that time, a progress bar appears that shows the progress of the script execution.

14 After script execution, summary details display for the total job and each server. An ID number at the top of the page identifies the job.

- To see script output, summary details and information about errors that might have occurred, click **View Details**.

- For each server, you can click **Download** to obtain a zip file (`results.zip`) that contains script execution output and error data.

The data is in two files called `stdout` (output data) and `stderr` (error data), in a directory named `<servername>`. For example, for a server named `m0043`, the output and error files would be located as follows: `m0043/stdout` (output file for server named `m0043`) and `m0043/stderr` (error file for server named `m0043`).

15 Click **Close** to exit the wizard.

Script Execution Results

This section provides information about script execution results and contains the following topics:

- Viewing Execution Results Immediately After Script Execution
- Viewing Execution Results Stored in Opsware SAS

During execution, the current status of script execution events at each server displays on the Run Script page. When script execution activities finish, the page immediately displays a summary of execution results for each server and for the entire run. See Figure 11-10.

Figure 11-10: Script Execution Progress Page

Run Script - ID: 67490007
Please wait while the script is being run on the specified servers.

Running Script Complete
Status: 2 of 2 servers completed. [Download..](#)

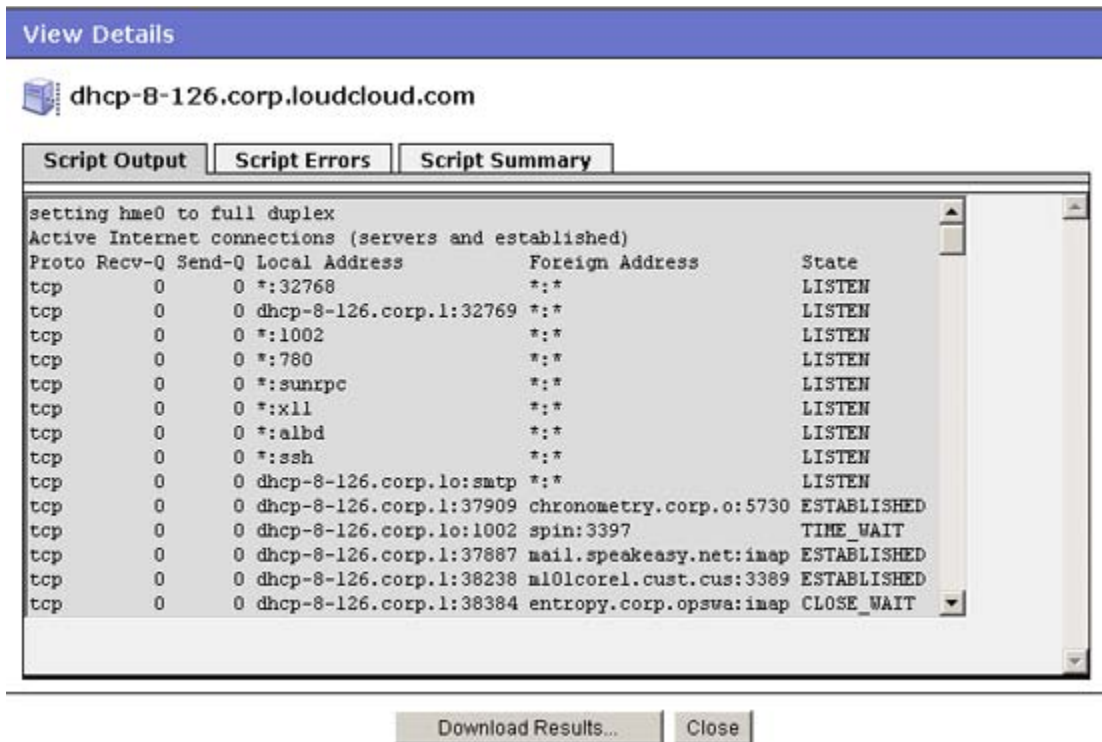
dhcp-8-126.corp.loudcloud.com <div style="text-align: right;">100%</div> View Details... Status: Running Script Complete
dhcp-8-130.corp.loudcloud.com <div style="text-align: right;">100%</div> View Details... Status: Running Script Complete

Script execution data and information are stored in the Model Repository and are later accessible through the My Jobs feature for the user who performed the execution.

Viewing Execution Results Immediately After Script Execution

After a script runs, execution data and information for a specific server are available by clicking **View Details** for that server. Information that is displayed includes script execution output, errors (if there are any) and summary data (such as the script name and contents, and the date of the run). See Figure 11-11.

Figure 11-11: Execution Results After Script Execution



A zip file (`results.zip`) is available that contains standard script execution output and error data in two files (`stdout` and `stderr`), which are located inside a directory name `<servername>`. You can download the zip file by clicking **Download**.

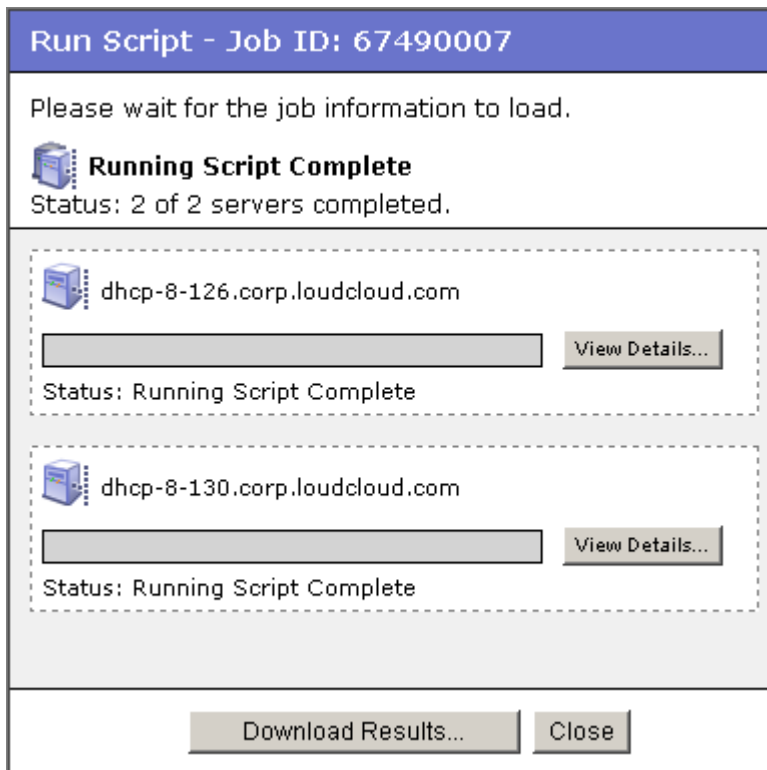
Viewing Execution Results Stored in Opware SAS

After script execution, script data results are available through the My Jobs feature.

The My Jobs list is available either at the My Jobs panel (SAS Web Client home page) or the My Jobs page (opened by clicking the My Jobs link at SAS Web Client's navigation panel). In the list, executed scripts are identified from other types of Opware SAS jobs by the name Run Script.

You can view Information about a specific executed script (started on a particular day and time) by clicking the Run Script link for the specified day and time. See Figure 11-12.

Figure 11-12: Execution Results for a Particular Script Execution Event



Script results data are held in the Model Repository for a limited amount of time (30 days, for example). The Opware administrator can configure this time period.

Error Resolution for Script Execution

The following section describes the events that might occur during Script Execution feature activities and provide suggestions for resolving the problems. This section contains the following topics:

- Resolving Script Uploading Errors
- Resolving Script Time-out Events
- Investigating Script Non-Zero Return Codes
- Investigating Server Authentication Errors
- Investigating Partial Executions

Resolving Script Uploading Errors

If errors occur when a user uploads a script, the SAS Web Client error pages display information about the event.

If errors occur, perform the following steps:

- The maximum size for a script is 4 MB. Verify that the script being uploaded does not exceed this size.
- If communication with the SAS Web Client is lost during the script upload process, upload the script again.

Resolving Script Time-out Events

When a script runs on an Opware-managed server, if the script hangs or is not finished before the script time-out value is reached, an Opware SAS error occurs and the script is stopped on the server.

The script time-out value is entered on the Specify Options page of the Run Distributed Script Wizard. The time-out value is the amount of time before a script times out.

Check that the length of time it takes for script execution does not exceed the current time-out value. Creation of debug output can also be added into the script for troubleshooting purposes. If the time-out event is due to the script hanging, then further examination of the script and server should occur.

Investigating Script Non-Zero Return Codes

If execution of a script on an Opware-managed server returns a non-zero code, an error is reported. (A zero return code indicates successful – for example, normal – operation.) Information about the error is available to the user immediately following the error event and script execution. Information is also available after execution through the My Jobs feature.

Depending on how a script is written, a non-zero return code might indicate a fatal error.

Investigating Server Authentication Errors

If an authentication error occurs at an Opware-managed server, verify that the user correctly enters the password. Also, verify that the correct user name and password are being used.

If authentication fails during execution of a script, an Opware SAS error is raised for the server running the script. Information about the error is displayed in the SAS Web Client for that server during and immediately following script execution. Script execution information is also available through the My Jobs feature.

Investigating Partial Executions

If a script runs on only some of the selected servers, this might be due to an Opware Command Engine failure or because someone else has locked the managed servers by, for example, running another Opware SAS task that uses the servers. Or, the servers might be unreachable.

Opware SAS Custom Extensions

Opware, Inc. Professional Services can extend functionality for customers by creating custom extensions to Opware SAS. Opware Custom Extensions (which are custom Command Engine scripts) extend Opware SAS functionality to cover specific customer needs.

In Opware SAS, the Command Engine is a system for running distributed programs across many servers (utilizing the Opware Agents running on the servers). Opware SAS features, such as the Code Deployment feature, use Command Engine scripts to implement part of their functionality

The Custom Extension feature is accessed through the Run Custom Extension Wizard. This Wizard allows a user to choose a custom extension to run, specify necessary input data for the extension, validate the data required to run the extension, run the extension, and view or download the results from the job. When a user runs a custom extension, the job shows up in My Jobs.

When a custom extension is added to one facility, it is automatically propagated to the other facilities in the multimaster mesh of Opsware SAS facilities.

To access the Run Custom Extension Wizard, users must be assigned to a user group that has the permission Wizard: Opsware Extension. When users have this permission, they can run any custom extensions on the servers they have access to in the SAS Web Client.

Running a Custom Extension

To run a custom extension, perform the following steps:

- 1** From the SAS Web Client home page, click the Run Custom Extensions link in the Tasks panel.

Or

From the navigation panel, click Servers ► Manage Servers. The Manage Servers list appears. Select the servers on which you want to run a custom extension and choose **Run Extension** from the **Tasks** menu.

The Run Custom Extension Wizard appears.

- 2** Select the custom extension that you want to run and click **Next**.

If you have already selected servers from the Manage Servers list, you must ensure that the custom extension that you select can run on the operating systems of the selected servers. Otherwise, an error message appears in this page and you cannot proceed.

Some custom extensions do not require that you select servers from the Server list. For example, the extension might prompt you in the Specify Settings step to enter server host names in a text box. If you already selected servers from the Servers list, an error message appears in the page.

If you have not already selected servers from the Manage Servers list, the Select Servers page appears.

- 3 If prompted, select the servers or groups on which you want to run the custom extension and click **Next**. You can find the servers that you want to run a custom extension on by browsing the list or by searching.

The Specify Settings page appears. See Figure 11-13.

Figure 11-13: The Specify Settings Page of the Run Custom Extension Wizard

Run Custom Extension

Specify Settings

Enter values for each field (**bold** items are required) to run this extension. Mouse over the note icon (📝) for directions on setting the values correctly.

Change_Password

Username: 📝

Current Password: 📝

Confirm Current Password: 📝

New Password (at least 8 characters with a digit): 📝

Confirm New Password (at least 8 characters with a digit): 📝

Run as root (Unix) or Administrator (Windows)?: Yes No 📝

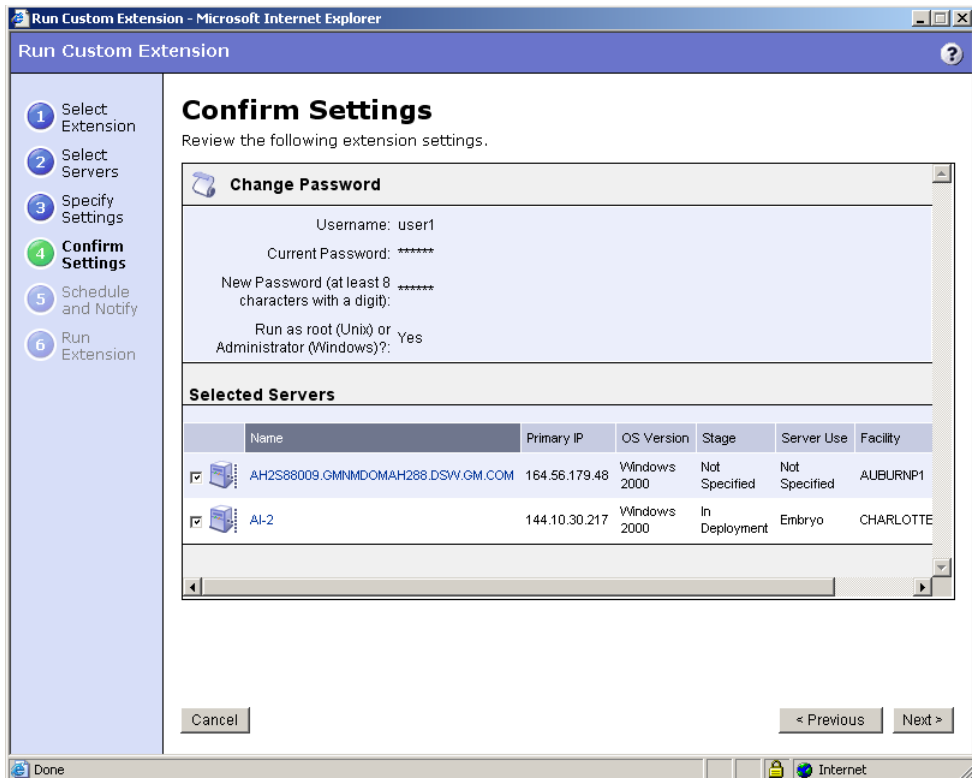
Cancel < Previous Next >

- 4 Specify the settings for the custom extension and click **Next**.

The settings that appear in the page are unique to the custom extension that is being run. For information about what data to enter in a field, move your mouse pointer over a Note icon.

The Confirm Settings page appears. See Figure 11-14.

Figure 11-14: The Confirm Settings Page of the Run Custom Extension Wizard



- 5 Review the values that you entered and the servers that you selected on which to run the custom extension. (You can remove servers from the list by deselecting their check boxes. The list displays the first nine servers on which the custom extension will run. Click the “Show remaining servers” link to display the complete list of selected servers.)
- 6 Click **Next**.
- 7 On the Schedule and Notify page, you have the following options:
 - **Notify:** Choose the Condition option and set the parameters to send an email when the operation is completed. You can choose to have an email sent on any result, if the operation fails, or if the operation is successful. To add another email recipient, click the plus (+) button next to the Recipients field.
 - **Schedule:** Choose either **Run Now** to execute the operation immediately, or choose **Specify Time** to schedule the operation for a later time.

When you schedule a job for a server group, you can specify how the members of the group are determined. The membership of a dynamic server group changes based on the changes in your operational environment. If you have "Allow Run Refresh Jobs" permissions, you will see additional options. Select either of the following options:

- **Option 1:** Membership is determined based on the "Time of Confirm Selection." Select this option to run the job on the servers that were in the group when you scheduled the job. Changes to the group membership do not affect the list of the servers that the job will run on.
- **Option 2:** Membership is updated when the job runs. Select this option to recalculate the group membership prior to running the job. Changes to group membership are reflected in the list of servers that the job will run on.



The time used for the scheduled job is specified in your preferred time zone which can be modified in My Profile. If you do not have the preferred time zone set, the time zone is derived from the Opware SAS core server (usually UTC).

8 Click **Run** to start the Custom Extension Wizard.

If you selected to run the job at that time, a progress bar appears for the servers on which the extension is running that shows the progress of the job. Depending upon how the custom extension was written, you will see the progress displayed in one of two ways:

- If the custom extension was written to show progress and status for individual servers, you will see individual progress bars for each server. When the custom extension has finished running, you will see the **View Details** button. You can click **View Details** to display detailed error information.
- If the custom extension was written to show progress for all servers, then you will see a single progress bars for all servers. When the custom extension has finished running for all servers, you will see **View Details**. You can click **View Details** to display detailed error information.

If an error occurs while the custom extension is running on servers, the progress bar moves to 100% and an error message appears below the bar.

For any servers where the custom extension has failed to run, you will have to either re-launch “Run Custom Extension” from the home page and pick the servers you want to try again or choose those servers from a Manage Server ► My Servers ► Server Search list and choose the menu item **Run Custom Extension**.

- 9** (Optional) When the custom extension finishes running, you can click **View Details** to see the results.

The Custom Extension Results window appears. The tabs in the window can vary depending on how the custom extension was implemented. To download the results to a file, click the download link. When you are done viewing the results, click **Close** to close the window.

- 10** Click **Close** to end the wizard.

Closing the wizard does not stop the custom extension if it is still running. After you close the wizard, you can view the progress of the running custom extension by viewing My Jobs (accessible from the Home page or the navigation panel). Each custom extension job is identified with the name Run Custom Extension. Click the name link to identify which extension was run.

See “Server Management Scheduling and Notification” on page 330 in Chapter 8 for information about the My Jobs feature.

Chapter 12: Code Deployment and Rollback

IN THIS CHAPTER

This section discusses the following topics:

- Opsware Code Deployment Process
- Services, Synchronizations, and Sequences



You must have specific permissions to deploy code and content by using the SAS Web Client. Contact your Opsware administrator to obtain the necessary access rights. For more information, see the Permissions Reference appendix in the *Opsware[®] SAS Administration Guide*.

Opsware Code Deployment Process

This section provides information on the code deployment process within Opsware SAS and contains the following topics:

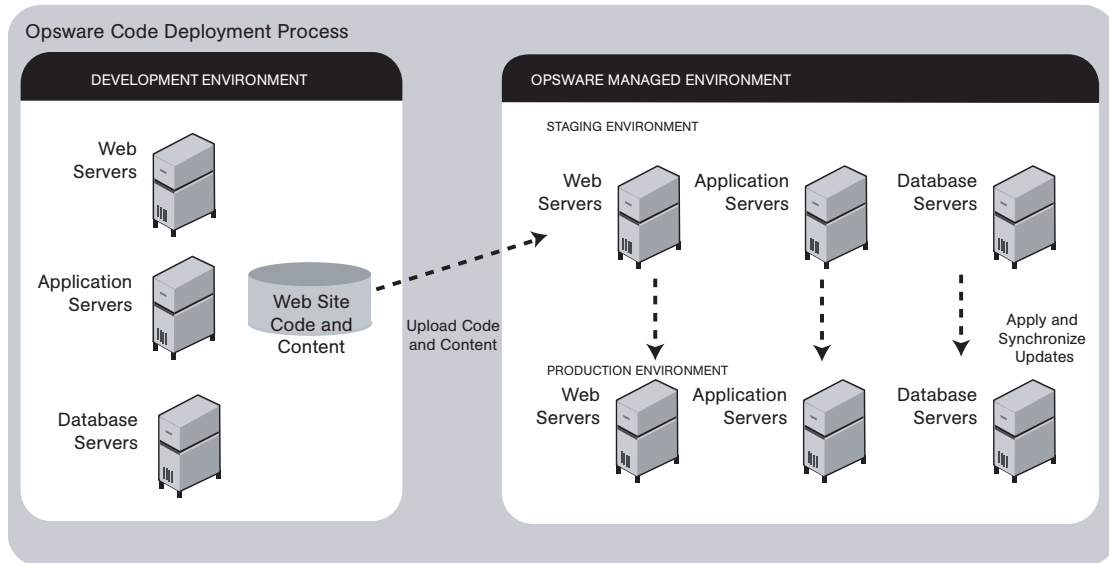
- Deploying Code
- Uploading Code and Content to Staging
- CDR Operations and Directories
- CDR Features
- CDR Permissions
- Accessing CDR

Deploying Code

The Code Deployment & Rollback (CDR) feature in the SAS Web Client provides tools for deploying new and updated code and content to your operational environment.

The following figure shows the architecture and process for updating a typical server hosted in an Opware managed environment.

Figure 12-1: Typical Code and Content Update in the Opware Managed Environment



The deployment process involves performing the following high-level tasks:

- 1** Determining your application code and content deployment requirements and defining the CDR services, synchronizations, and sequences that you need to support them.
 - Services are defined for each different type of web server or application server applications (for example, WebLogic Server) that is installed on the staging and production hosts in your environment.
 - Synchronizations are defined for each service so that you can update files between the source location and one or more destination production hosts that are running the same service.
 - Sequences are optional but can simplify deployment by grouping a collection of service operations and synchronizations that can be performed as a single task.
- 2** Uploading new or updated code and content to your Opware staging environment.
- 3** After performing any necessary testing, cutting over to the changed code and content on the staging environment.

- 4** As necessary, performing CDR service operations, such as backing up code and content from your live site.
- 5** Performing CDR operations available to synchronize the updated code and content to your production hosts in the Opsware managed environment.
- 6** To simplify subsequent deployments of new code and content, defining sequences that specify a series of service operations and synchronizations you want to perform as a single action.



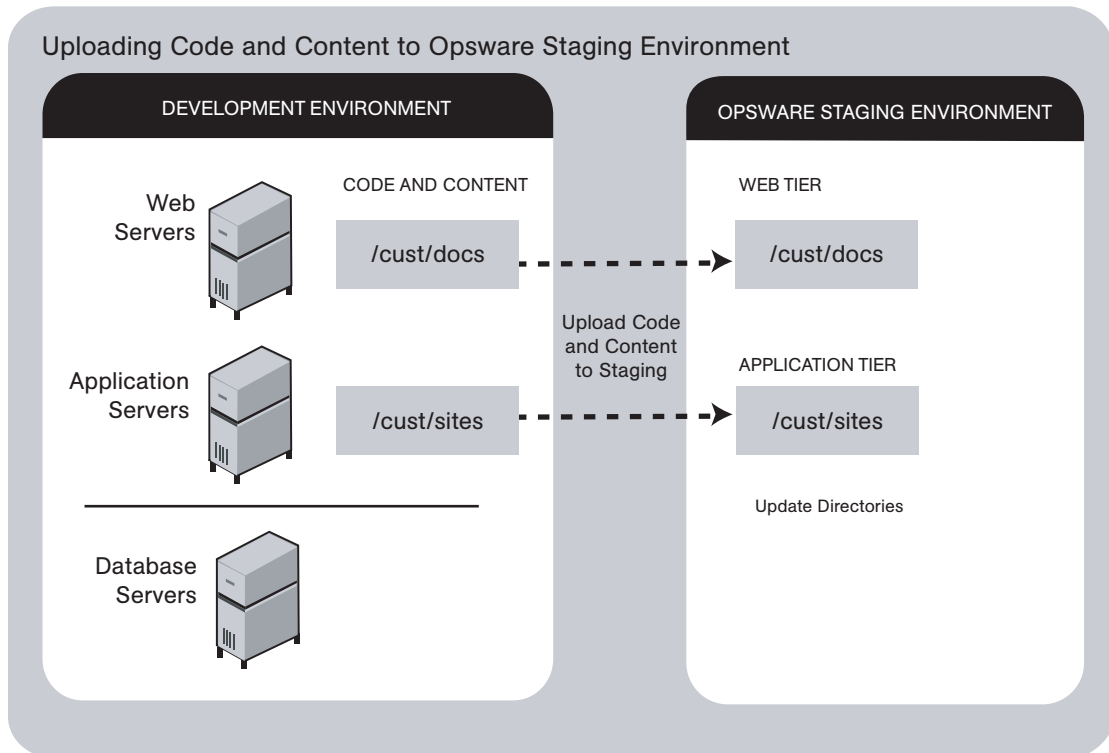
The code and content deployment process that you follow might be different depending on the architecture of your operational environment and your deployment requirements.

Uploading Code and Content to Staging

Before you use CDR to push code and content, you must upload new or updated files to your Opsware staging environment. You can use content management tools, such as OpenDeploy, scp, or rsync over SSH, to do that.

The following figure shows an example of a typical development environment and how your uploaded code and content move to the staging environment.

Figure 12-2: How Code and Content Move to the Staging Environment



After you upload the files and test your changes, you can synchronize updates to the production hosts running your managed environment. You can run specific synchronizations and perform other service deployment operations by selecting CDR menu options available from the SAS Web Client navigation panel.

CDR Operations and Directories

After you upload updated code and content to your Opware-managed staging environment, you can use the CDR operations to cutover to new code and content, perform host synchronizations, and perform other service operations.

CDR uses the following directories to synchronize and cutover code and content for specified hosts:

- **Live directory:** The directory that stores the actual code and content required to run a live site.

- **Update directory:** The directory written to by CDR synchronizations. Stores only the files that changed between the source host Live directory and the Live directories of the destination hosts.
- **Site Previous directory:** This directory holds all the changes necessary to revert the Live directory back to the state it was in before the last cutover. Like the Update directory, the Site Previous directory only stores the files that changed between the current Live directory contents and its previous state.
- **Site Backup directory:** This directory stores a complete backup of the site. The directory is populated when the user issues a Backup service operation.

When you cutover to new code and content, CDR determines the differences between the new code and content in the current Update directory and the Live directory for your site. The files that are different are synchronized to the Live directory. When you synchronize source and destination hosts, CDR moves modified files from the Live directory on a source host to a directory on a destination host.



You cannot use CDR to automate database pushes. However, you can configure CDR so that you can synchronize modified database script files on different hosts.

CDR Features

CDR offers the following features:

- Provides a single tool for deploying code (such as ASP, JSP, and JAR files) and site content (such as HTML, JPEG, GIF, and PDF files). Using a single tool is helpful when the code and content for your site are intermingled.
- Provides direct control over code and content pushes by making it possible to decide what information to update and determine when and how to perform updates.
- Provides flexibility to accommodate frequent updates to staging and production hosts by enabling more frequent pushes in a shorter period of time.
- Allows verification of file changes between staging and production host directories by creating a manifest of updated files. You can verify changes before cutting over to new code and content.
- Provides administrative service operations, including starting and stopping services, and backing up, restoring, and rolling back code and content to return your site to the previous version.

- Lets you push incremental updates to your site so that only files that have changed are pushed to specified locations on staging or production hosts.
- CDR uses the same authentication and navigation that you use in accessing other information and performing other site operations from the SAS Web Client.

CDR Permissions

As with all other features in Opsware SAS, the links that you see on the SAS Web Client Home page and the links that you see in the navigation panel are based on the permissions that you have in combination with the customer you are associated with.

If you do not have permissions for CDR, you cannot see the Code Deployment links on the navigation panel, the link called Deploy Code in the Tasks panel of the SAS Web Client home page appears in italics, and it is not an active link.

If you have CDR permissions to no more than one customer, when you expand the Code Deployment section in the navigation panel, you can see a link called Set Customer. Click that link to view the links to the specific Code Deployment functions that you have permissions for in combination with that single customer.

If you have CDR permissions to more than one customer, you can see a link called Select Customer. Click that link to display a page that shows the customers you are associated with. Select the customer you want to work with. The CDR Home Page appears, with links to the specific Code Deployment functions that you have permissions for. These links are the same functions that you can find in the navigation panel under Code Deployment.



The navigation instructions and screen captures in this chapter show what a user with permissions to all code deployment functions and access to only one customer can see. Consequently, because your permissions and customers might be different, the available menu selections and features that you see might likewise differ.

Accessing CDR

Perform the following steps to access CDR:

- 1 If necessary, click the Code Deployment link in the navigation panel to expand the list of CDR options.
- 2 Click the CDR Home link. The CDR Home Page for [customer name] appears, as the following figure shows.

Figure 12-3: Code Deployment Home Page

CDS Home Page for Main Customer	
LINK	DESCRIPTION
Service Management	Create, Modify, and Delete Service Definitions. Services define the location and commands to manipulate an application on hosts.
Run Service	Perform a service operations on one or more hosts, or request that a service operation be performed on your behalf. Service operations include starting or stopping applications, cutting over or rolling back code, and backing up or restoring code.
Sync Management	Create, Modify, and Delete Synchronization Definitions. Synchronizations define the path for pushing code from a source service host to one or more destination service hosts.
Synchronize	Perform a synchronization to one or more hosts, or request that a synchronization be performed on your behalf.
Sequence Management	Create, Modify, and Delete Sequence Definitions. Sequences allow the grouping of service operations and synchronization operations to define higher level code deployment operations.
Run Sequence	Perform a pre-defined sequence of service operations and/or synchronizations on one or more hosts, or request that a sequence be performed on your behalf.
View History	Get information about previously run Code Deployment Operations.

Depending on your access permissions, the following CDR options appear:

- **Service Management:** Create, modify, or delete service definitions that define the location and commands to manipulate an application on hosts associated with each application instance running in your operational environment.

- **Run Service:** Perform a service operation or request that one be performed.
 - **Sync Management:** Create, modify, or delete synchronization definitions associated with code pushes.
 - **Synchronize:** Perform a synchronization or request that one be performed.
 - **Sequence Management:** Create, modify, or delete sequences of operations.
 - **Run Sequences:** Perform a selected sequence or request that one be performed.
 - **View History:** View information stored in an operations log to determine the status of particular deployment operations, and whether they completed successfully.
- 3** Choose the CDR operations that you want to perform, selecting options from the navigation panel or from the CDR home page.

Services, Synchronizations, and Sequences

This section provides information on performing services, synchronizations, and sequences within Opsware SAS and contains the following topics:

- Overview of Performing Services, Synchronizations, and Sequences
- Synchronization of Site Code and Content
- Performing Synchronizations
- CDR Cutover Operation
- CDR Service Operations
- Starting and Stopping Host Services
- Backing Up Code and Content
- Restoring Code and Content from a Previous Version
- Rolling Back Code and Content to the Previous Version
- Accessing Service Operations in CDR
- Performing Service Operations by Service Name
- Performing Service Operations by Host Name
- Performing Sequences
- Processing Code Deployment Requests from Users

- Status View of Previous Operations

Overview of Performing Services, Synchronizations, and Sequences

After you upload updated code and content to your Opsware SAS staging environment, you use CDR to cutover to new code and content, perform host synchronizations, and perform other service operations.

When you cutover to new code and content, CDR determines the differences between the new code and content in the current Update directory and the Live directory. The files that are different are synchronized to the Live directory. When you synchronize source and destination hosts, CDR moves modified files from the Live directory on a source host to a directory on a destination host.

The code and content footprint that CDR maintains on a host is larger than the storage space for the code and content files of the live site. The amount of storage used beyond the actual size of your site increases with the number of files that you modify and back up.

Synchronization of Site Code and Content

CDR uses the following directories to synchronize and cutover code and content for specified hosts:

- **Live directory:** The directory that stores the actual code and content required to run a live site.
- **Update directory:** The directory written to by CDR synchronizations. Stores only the files that changed between the source host Live directory and the Live directories of the destination hosts.
- **Site Previous directory:** This directory holds all the changes necessary to revert the Live directory back to the state it was in before the last cutover. Like the Update directory, the Previous directory only stores the files that changed between the current Live directory contents and its previous state.
- **Site Backup directory:** This directory stores a complete backup of the site. The directory is populated when the user issues a Backup service operation.

CDR can synchronize updates from the Live directory of a source host to either the Update or Live directories on destination hosts. Decide whether you want to synchronize changed files on the source host to Update or Live directories on the destination hosts:

- **Synchronize to Update directories:** CDR determines files that have changed by comparing files in the destination host Live directory and the source host Live directory. Updated files are stored in the Update directories of destination hosts.
- **Synchronize to Live directories:** CDR updates changed files to the Live directory on destination hosts bypassing the Update directory.

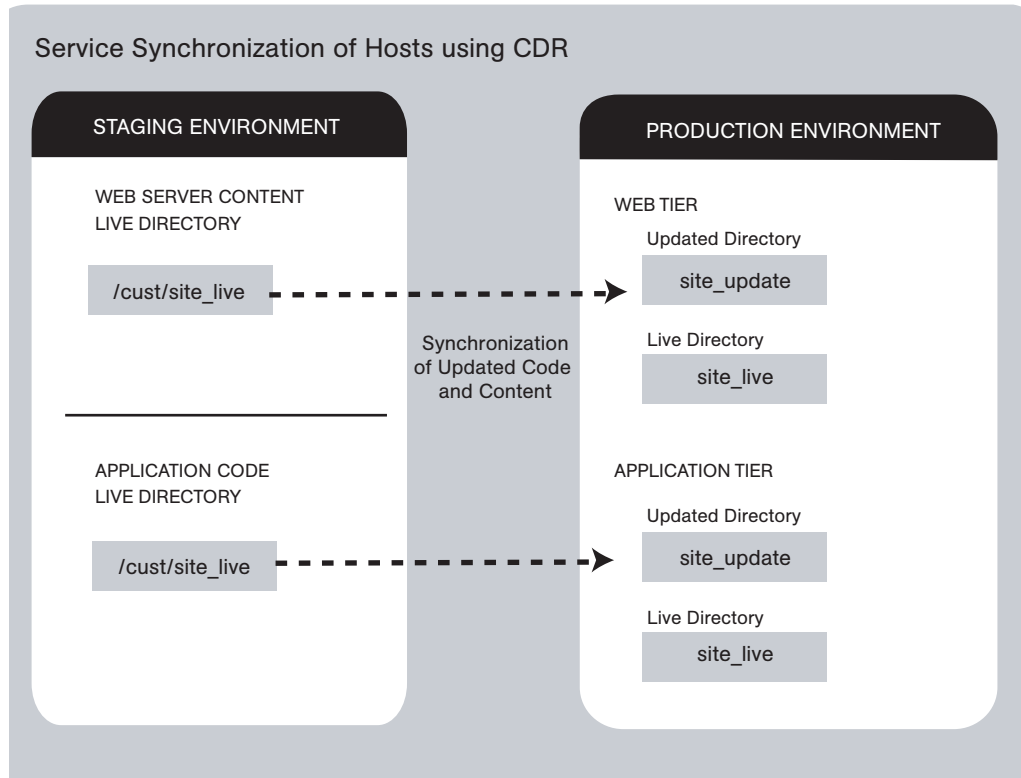


If you choose to synchronize directly to Live directories, the Rollback operation does not function properly. Therefore, choose this option only for synchronizations that are not likely to impact site stability.

When you choose to synchronize to Live directories, back up the Live directories first and run the Restore operation to return your site to the previous version. See “Rolling Back Code and Content to the Previous Version” on page 451 in this chapter for more information.

Figure 12-4 shows an example of synchronization between hosts and how you synchronize updates for each service.

Figure 12-4: Service Synchronization of Hosts Using CDR



Contact your Opsware administrator for a description of services and synchronizations set up for your site and the specific operations that you need to run when updating code or content for a particular host service.

Performing Synchronizations

Perform the following steps to synchronize updated code and content from one source host to one or more destination hosts:

- 1** Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
- 2** Click the Synchronize link.

A page appears that displays the synchronizations that you can perform.

- 3 Select the synchronization that you want to perform by clicking the link. The CDR Synchronize for [customer name] page appears, as Figure 12-5 shows.

Figure 12-5: The CDR Synchronize Page

- 4 Select one or more of the displayed host names on which you want to perform synchronization. The hosts that you select are the destination hosts.



Choose the Select/Deselect All option to select all or clear all host names.

- 5 (Optional) To view a list of files that will be created, modified, and deleted on the destination hosts, click **Preview**.
Or
(Optional) To view a list of all the files on the destination hosts, click **List**.
- 6 Select the Perform Operation option to directly perform a selected synchronization.

Or

Select the Submit Request To option to send a request to users specified to receive email notification for service and synchronization requests. When you submit a request, specify any additional instructions that you want to include for the requested synchronization. For example, these might be instructions such as the time that you want the synchronization performed, verification, or other related services to perform.



The Perform Operation option is only visible when you are a member of an SAS Web Client user group allowed to directly perform a synchronization.

7 Choose the type of synchronization that you want performed from the drop-down list:

- Synchronize To Update
- Synchronize To Live

See “Synchronization of Site Code and Content” on page 443 in this chapter for information about these options.

8 To initiate the synchronization or send the request, click **Run**.

CDR Cutover Operation

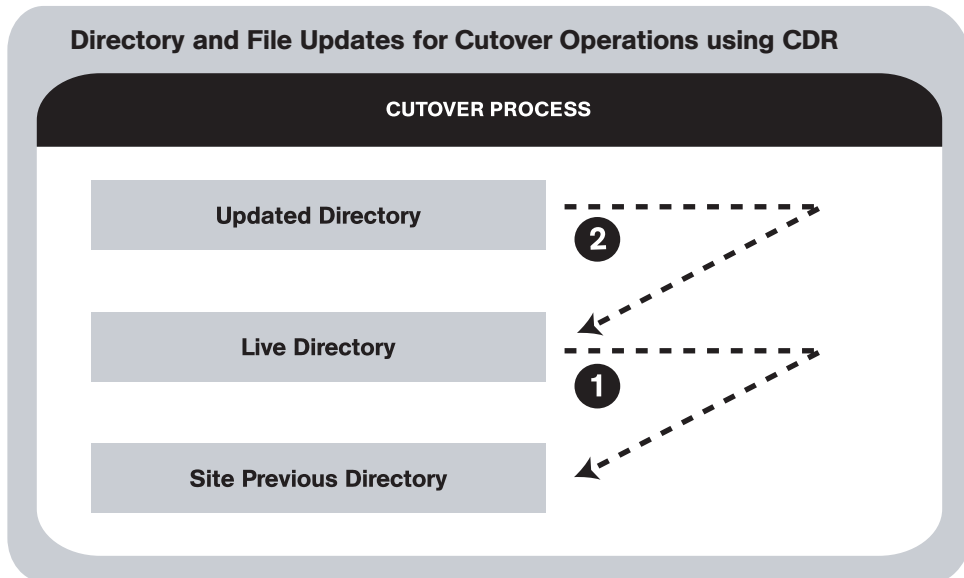
Perform the cutover operation to make the Update directory and the current live site identical.

When you cutover, CDR performs the following actions:

- Updates the Site Previous directory with files from the Live directory. CDR saves modified files and files-to-be-deleted to the Site Previous directory. The Site Previous directory contains the files necessary to restore the live site to the previous version.

- Determines the differences between the Update directory and the current Live directory. The files that are different are synchronized from the Update directory to the Live directory. See Figure 12-6.

Figure 12-6: Directory and File Updates for Cutover Operations Using CDR



CDR determines file differences between source and destination directories based on file size, modification date and time, ownership, group attributes, and permissions attributes.

By using the cutover process, CDR ensures your ability to rollback to the previous version of your code and content if you experience a problem.

Your Opsware administrator can configure a CDR service to run scripts before and after cutting over to updated code and content. For example, before and after cutting over, you might distribute content on geographically disperse servers.

See "Synchronization of Site Code and Content" on page 443 in this chapter for information about a description of these directories. See "CDR Service Operations" on page 449 in this chapter for information about how to rollback code and content to the previous version.

CDR Service Operations

In addition to the Cutover operation, CDR provides a number of service operations:

- Starting and stopping host services
- Backing up code and content
- Restoring code and content from a previous version
- Rolling back code and content to the previous version

Performing these operations might be required depending on the type of code and content changes made or the host services that are affected.

The operations that you need to perform are specific to the service (for example, Web server or application server instance) for which you are updating code or content and the particular host.

Starting and Stopping Host Services

Stopping and starting services might be required depending on the type of code and content changes made or the host services that are affected. Discuss your requirements with your Opsware administrator.

Typically, you only stop and start host services for the hosts in your staging environment. Select members of your staff, or other individuals in your operations center, can stop and start host services for the hosts in your production environment.

Start: Launch a defined service; for example, starting a web or application server instance that is running on a specific host.

Stop: Shut down a defined service; for example, shutting down a web or application server instance before cutting over to new or changed code and content on a specific host.

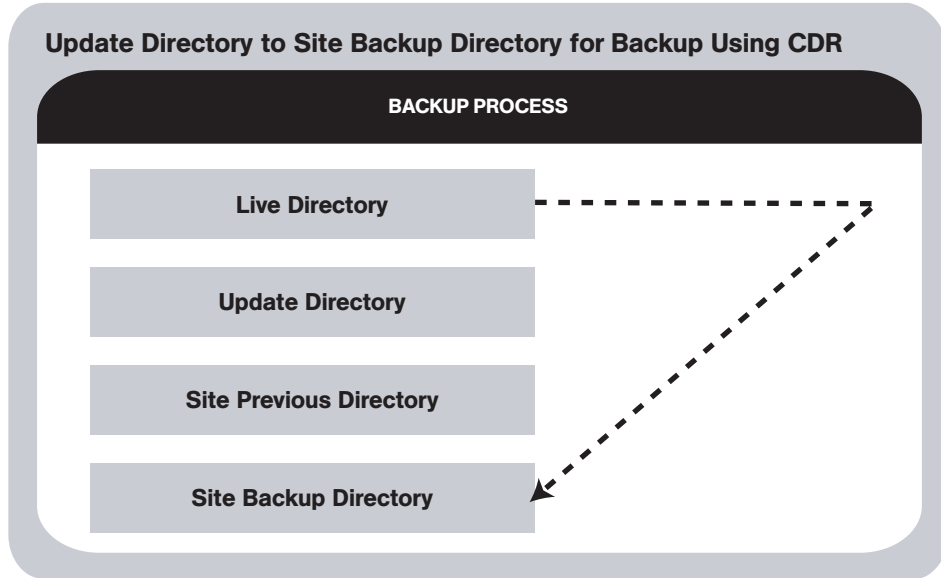
Backing Up Code and Content

When you use CDR to back up your site, CDR saves the entire contents of the current Live directory for a specific service in the Backup directory. CDR saves the backup copy to the local disk for the host on which you ran the Backup operation. See Figure 12-7.



You can use CDR to keep only one backup copy at a time for a service.

Figure 12-7: Update Directory to Site Backup Directory for Backup Using CDR



When you run the Restore operation, CDR replaces the Live directory contents with files stored in the Backup directory.

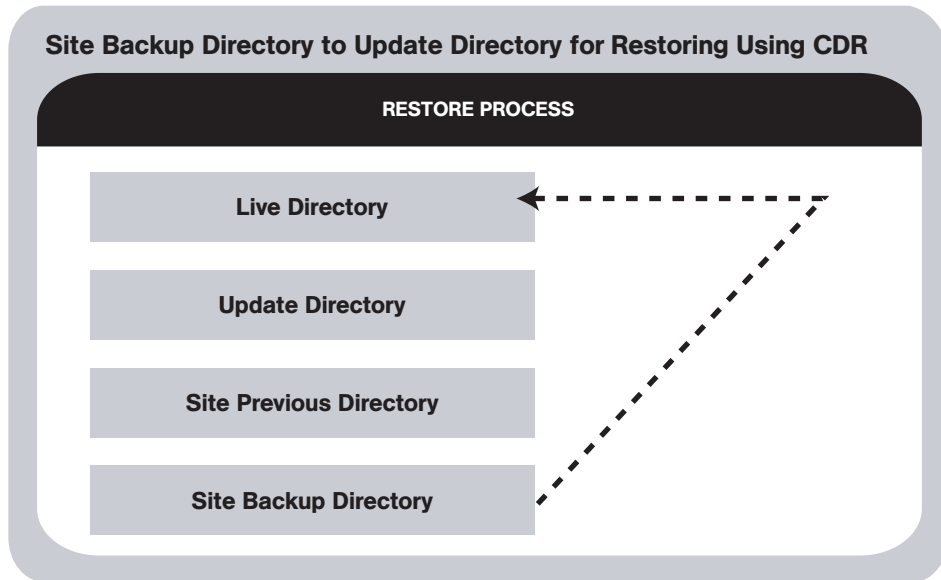


When you reach a high level of site stability, backing up your site is recommended, especially if you plan to make changes to site code and content.

Restoring Code and Content from a Previous Version

The Restore operation restores the previous Live directory by copying the contents of the Backup directory to the Live directory. Restoring code and content from the Backup directory does not change files that are stored in the Update directory. See Figure 12-8.

Figure 12-8: Site Backup Directory to Update Directory for Restoring Using CDR



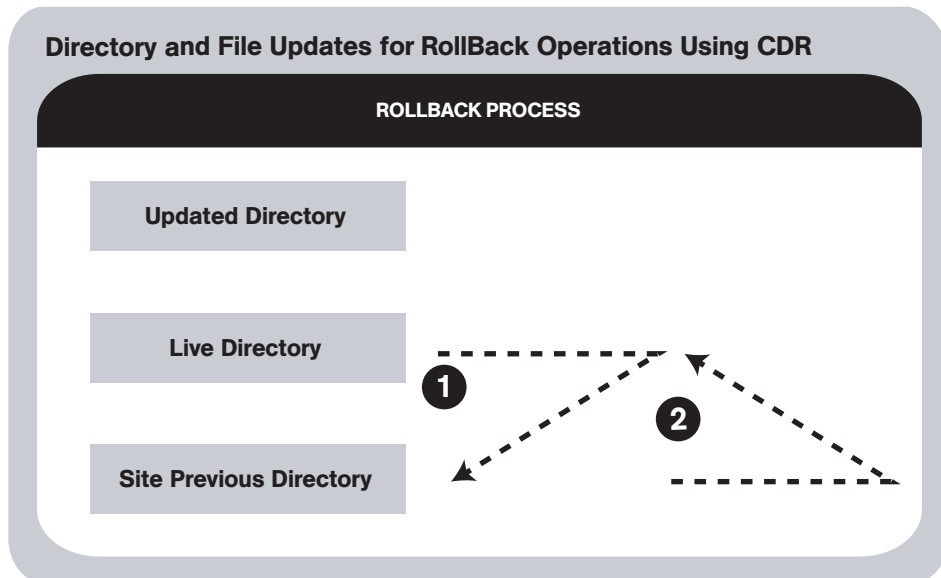
Before you restore code and content, you must have backed up the contents in the Live directory to the Backup directory by performing a Backup operation.

Rolling Back Code and Content to the Previous Version

If you experience a problem after cutting over updated code and content to your production site, you can rollback to the previous version.

Rolling back returns the site to the state it was in prior to the last cutover that you performed. See Figure 12-9.

Figure 12-9: Directory and File Updates for Rollback Operations Using CDR



During cutover, CDR updates the Site Previous directory with files from the Live directory. CDR saves modified files and files-to-be-deleted to the Site Previous directory. The Site Previous directory contains the files necessary to restore the live site to the previous version.

During rollback, CDR restores the set of different files (modified files and files that were deleted during cutover) to the Live directory.



If you upload files directly to the Live directory or choose to synchronize directly to Live directories, the rollback operation does not function properly. Under these conditions, back up your Live directory and run the Restore operation to return your site to the previous version.

Accessing Service Operations in CDR

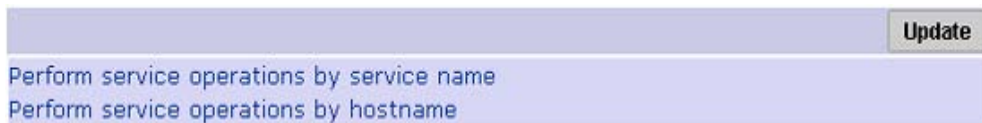
The Service Management option provides a number of service or administrative operations, including starting and stopping host services, backing up, restoring, or rolling back code and content, and cutting over to new site code and content.



To access CDR, your Opsware administrator must add you as a member of a user group authorized to use CDR.

You have the option of initiating a service either by selecting a service name or by selecting host names. You must select both a service to perform and the hosts on which to perform the service. See Figure 12-10.

Figure 12-10: Run Service Page



- Initiate a service by selecting the “Perform service operations by service name” option first when you want to perform a service on multiple hosts at the same time. Selecting the service name first shows you all the hosts for which that service is defined.
- Initiate a service by selecting the “Perform service operations by host name” option first when you want to perform a service on a single host or on a specific host where you know the host name. Selecting the host name first shows you all the services that are defined for that host.

Performing Service Operations by Service Name

Perform the following steps to perform service operations by service name:

- 1** Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
- 2** Select the Service Management option.
- 3** From the Service Management page, select the “Perform service operations by service name” link.

- 4 Select a service from a list of services defined for your site. A page that prompts you to select the hosts and the operation that you want to perform appears, as Figure 12-11 shows.

Figure 12-11: Perform Service Operations by Service Name Page

- 5 Select one or more of the displayed host names. You can choose the Select/Deselect All option to select all or clear all host names for the operation that you want to perform.
- 6 Select the Perform Operation option to directly perform a selected operation.



The Perform Operation option is visible only when you are a member of the CDR user group that allows users to directly perform a service operation.

Or

Select the Submit Request To option to send a request for authorized individuals to perform the operation for you. When you submit a request, specify any additional instructions that might be required to perform the requested operation.

7 Choose the type of operation that you want performed from the drop-down list:

- Start
- Stop
- Cutover
- Rollback
- Backup
- Restore

See “CDR Service Operations” on page 449 in this chapter for information about these operations.

8 To initiate the operation or send the request, click **Run**.

Performing Service Operations by Host Name

Perform the following steps to perform service operations by host name:

- 1** Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
- 2** Select the Service Management option.
- 3** From the Service Management page, select the “Perform service operations by hostname” link.
- 4** Select a host name from the list of staging and production hosts available for your site. A page that prompts you to select the service and the operation that you want to perform appears, as Figure 12-12 shows.

Figure 12-12: Perform Service Operations by Host Name Page

- 5** Select the service for which you want to perform an operation.
- 6** Select the Perform Operation option to directly perform a selected operation or select the Submit Request To option to send a request to have authorized individuals perform the operation for you. When you submit a request, specify any additional instructions that might be required to perform the requested operation.



The Perform Operation option is visible only when you are a member of the user group that allows users to directly perform a service operation.

- 7** Choose the type of operation that you want performed from the drop-down list:
 - Start
 - Stop
 - Cutover
 - Rollback
 - Backup
 - Restore

See “CDR Service Operations” on page 449 in this chapter for information about these operations.

- 8** To initiate the operation or send the request, click **Run**.

Performing Sequences

CDR also allows you to perform service operations and synchronizations that have been set up as a sequence of operations.

Perform the following steps to perform CDR sequences set up for your site:

- 1** Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
- 2** Click the Run Sequence link.

The CDR Run Sequence for [customer name] page appears that shows the sequences that you can run. See Figure 12-13.

Figure 12-13: CDR Run Sequence Page

Choose the Sequence You Wish to Perform/Request

Backup Prod Site
Push WebSite and App Code
Restore Production Site from Backup
Rollback Web & App Code

- 3 Select the sequence that you want to perform by clicking the link. The Run Sequence page appears, as Figure 12-14 shows.

Figure 12-14: Run Sequence Page That Shows Details of a Specific Sequence

<input type="button" value="Update"/>				
Step	Run	Service/Synchronization	Operation	Hosts
1	<input checked="" type="checkbox"/>	Apache Front End Service	Backup	r 010 dev.opsware.com
2	<input checked="" type="checkbox"/>	WebLogic App Server Service	Backup	r 010 dev.opsware.com
<input type="radio"/> Perform Operation <input type="radio"/> Submit Request To Perform				
Additional Information				
Extra Instructions		<input type="text"/>		
<input type="button" value="Run"/> <input type="button" value="Cancel"/>				

- 4 Select the Perform Operation radio button to directly perform the selected sequence.

Or

Select the Submit Request To Perform radio button to send a request to the users specified to receive email notification for service, synchronization, and sequence requests. When you submit a request, specify any additional instructions that you want to include for the requested sequence. For example, you might want to include instructions such as the time that you want the sequence to run, verification, or other related services to perform.



The Perform Operation option is visible only when you are a member of a user group allowed to directly perform a sequence.

- 5 To initiate the sequence or send the request, click **Run**.

Processing Code Deployment Requests from Users

When CDR users request that a service operation or synchronization be performed on their behalf, an email notification is sent to the individuals assigned to perform the requested service operation or synchronization.

The following message is a typical example of an email notification request.

```
From: CDR-tool@opsware.com
To: opscenter@opsware.com
Date: Tue, 10 Jul 2001 11:25:13 -0700
Subject: Request To Perform Start operation for opsware.com
```

Please perform the following request

```
Requestor: jhancock/opsware.com
Request Time: Jul 10, 2001 11:25:13 AM PDT
Requested Service: Demo Apache
Requested action: Start
Perform on the following hosts:
host1.opsware.com
host2.opsware.com
```

Extra Instructions:

In this case, the email message specifies a request from a user, jhancock, to perform a Start operation on two hosts running the Demo Apache service. The subject line provides a summary of the request. In addition, the email indicates the time that the request was sent.

Perform the following steps to process the request:

- 1** Identify any special instructions that might need to be carried out for the specific request.
- 2** Log into the SAS Web Client, choose the CDR option, and then select the particular option within CDR to perform the requested operation.
- 3** When you successfully complete the CDR request, you might want to notify the individual user making the request, and all other involved parties, that the requested operation was completed.

If you encounter problems in completing a request and cannot resolve them, contact your Opsware administrator for any specific remedies and follow normal escalation procedures defined for your operational environment.

See the *Opware® SAS Policy Setter's Guide* for more information about troubleshooting tips.

Status View of Previous Operations

CDR maintains a log of operations (service operations, synchronizations and sequences) that were executed. You can view this information to determine the status of particular deployment operations, and whether they have completed successfully. You can also use the My Jobs task area of the SAS Web Client Home page, or the My Jobs link to view this information.

Accessing the Log

Perform the following steps to access the log:

- 1** Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
- 2** Select the View History option.

CDR displays a page providing a list, most recent to oldest, of operations that are either in progress or those that have been completed. This information displays only for the past 60 days. Each page is limited to a list of 10 operations. A Next link displays at the end of the page if there are more than 10 operations to view. Click the Next link to view subsequent operations. A Previous link is available to return to previous pages.



You need to refresh the page to view the status of any operations initiated after you selected the View History link.

A similar page displays after you select the View History link. See Figure 12-15.

Figure 12-15: CDR View History Page

Most Recent Session History (Page 1 of 1)				Refresh
Session ID	Operation Name	Username	Status	Initiated Date
70340007	Rollback Web & App Code	cdsonly	SUCCESS	Thu Oct 16 18:29:03 UTC 2003
70310007	Push WebSite and App Code	cdsonly	SUCCESS	Thu Oct 16 17:49:24 UTC 2003
70300007	Push WebSite and App Code	cdsonly	INCOMPLETE	Thu Oct 16 17:46:50 UTC 2003
69810007	New Sequence	edwardc	INCOMPLETE	Wed Oct 15 20:34:11 UTC 2003

The individual headings of column information included in the table are:

- **Session ID:** A session is created each time a CDR operation is performed. Click the Session ID to view detailed results of the operation.
- **Operation Name:** The name of the service, synchronization or sequence as specified when they were first defined.
- **User Name:** The user ID of the user that initiated the operation.
- **Status:** This describes the state of the operation at the end of the sequence. The status message varies depending on the type of operation. Single step operations always result in Success/Failure messages while multiple step operations (Sequence operations) could result in Complete with Error, Incomplete, or Success messages. Table 12-3 describes the possible status messages.

Table 12-3: CDR History Status Messages

STATUS TYPE	DESCRIPTION
Abort	This message displays only if a CDR specific script that is executed in order to complete service, synchronization or sequences fails. Such issues should be escalated to your Opsware Support Representative.
Active	This message displays if an operation is still in progress.
Complete with error	The sequence completed successfully but there were errors reported while the operation was in progress and the user opted to continue rather than cancel the operation.
Failure	The operation (service, sequence or synchronization) did not complete successfully.
Incomplete	The sequence resulted in an error and the user opted to cancel the sequence rather than continue.
Success	The operation (service, synchronization or sequence) was completed successfully and no errors were reported. In the case of a sequence, this message means that all the steps were completed successfully.
Initiated Date	The date on which the operation was initiated.

Chapter 13: Configuration Tracking

IN THIS CHAPTER

This section discusses the following topics:

- Overview of Configuration Tracking
- Configuration Tracking Operations
- Customized Configuration Tracking Policies
- Manual Backups
- Backup History
- Restoration of Backed Up Files

Overview of Configuration Tracking

The Configuration Tracking feature of Opware SAS allows you to monitor critical configuration files and configuration databases. When Opware SAS detects a change in a tracked configuration file or configuration database, the system can perform a number of actions, including backing up the configuration file or sending an email to a designated individual or group. You use configuration tracking policies to identify the files to be tracked and actions to be taken when change is detected. A configuration tracking policy consists of one or more configuration tracking policy entries that specifies the configuration file, the directory of configuration files, or the configuration database that you want to track.

The Configuration Tracking feature is designed for flexibility. For example, you can set configuration tracking defaults for a particular software application, and all attached servers automatically get those defaults. You can also quickly deploy the common configuration tracking defaults to a large number of servers in your Opware managed environment or create a specific policy for a single server.

Configuration Tracking allows you to recover from many problems caused by changes to configuration files. Using Automated Configuration Tracking, you can identify which tracked configuration files have changed, thus helping you identify the potential source of a problem. If you back up your configuration files with the Configuration Tracking feature, you can quickly restore the changed configuration files to a previous version.

You can also view a detailed history of all backup activity. This history includes a list of all tracked files that have been backed up and what types of backups occurred. If the backed up configuration files are text-based, you can download the files from the backup history and compare them to determine what specific changes have been made.



The Configuration Tracking feature is not a general-purpose backup solution. Configuration Tracking is designed to monitor text-based configuration files and specific types of configuration databases. The number and size of files that can be monitored on any managed server is limited.

File Types Supported

You can use the Configuration Tracking feature with the following types of files:

- Text-based configuration files
- The COM + Registration Database (Windows 2000)
- The IIS Metabase
- Windows Registry keys

Configuration Tracking Operations

This section discusses the following topics:

- Change Detection
- Types of Actions Performed
- Types of Backups Performed
- Email Automated Configuration Tracking and Logging Actions
- Creating the Email Notification List

Change Detection

All servers that Opsware SAS manages have an Opsware Agent installed on them. On servers that use Configuration Tracking, every four hours the Opsware Agent inspects the configuration files and databases that you select to track.

The Opsware Agent computes an MD5 checksum to determine if the contents of a tracked file have changed. (Any change to the contents of the file results in a change to the MD5 checksum.) If the contents of the file have changed, the action that you specify in the tracking policy is performed. For example, if you create an entry in your tracking policy for the `/etc/passwd` file and select backup as the action to be taken, the file is backed up when the Opsware Agent discovers a change in the `/etc/passwd` file.

The creation or deletion of a tracked file (or files inside a tracked directory) also counts as change and triggers a policy's action. (There are some exceptions; see the *Opsware[®] SAS Policy Setter's Guide* for more information.)

Changes to the properties of a tracked file or directory (such as changes to permissions or time stamps) do not count as a change. When a file or directory is backed up, however, its properties are backed up as well.

The first time that a tracking policy is deployed, all targets are considered changed. The Opsware Agent is encountering the files for the first time, and all of the policy's actions are triggered.

Types of Actions Performed

Opsware SAS can perform the following actions when change is detected in a tracked configuration file or configuration database:

- Back up
- Send email to addresses specified in the policy entry
- Send email to a designated notification group specified by a custom attribute
- Create an entry in the server's standard system log, (the syslog on Unix servers and the event log on Windows servers)

Types of Backups Performed

If you selected backup as the action for a tracked configuration file, the two general types of backups that can occur are incremental backups and full backups.

Incremental Backups

During an incremental backup, only targets that have changed since the last backup (and that have been selected to be backed up) are backed up.

An incremental backup occurs automatically when the Opsware Agent detects change in a tracked file that is selected to be backed up. (The Opsware Agent checks for change every four hours.)

Incremental backups also occur before and after you restore a previous version of a backed up configuration file to a server. These backups allow you to rollback the restored files.

Full Backups

During a full backup, all tracked configuration files that were selected to be backed up are backed up, not just the files that have changed.

Once a week, the Opsware Agent on a server checks to see if any files have changed since the last full backup. If any files have changed, Opsware SAS performs a new full backup. If no files have changed, the full backup does not take place.

You can also force Opsware SAS to perform a full backup on a server by selecting the Perform Manual Backup option. (See "Manual Backups" on page 477 in this chapter for more information.)

See "Backup History" on page 477 in this chapter for information about Backup types.



Backups are stored in the Software Repository until you delete them. You should delete old backups periodically, especially if you are backing up a large number of files that change frequently. See "Deleting Backups" on page 484 in this chapter for information about the procedure for deleting backups.

Email Automated Configuration Tracking and Logging Actions

You can choose to have email sent when a monitored target changes. The following example shows the text of an email generated when a tracked file changed.

```
From: <configurationtracking@yourcompany.com>  
Date: Thu Jan 16, 2003 5:40:11 PM US/Pacific  
To: <joe@yourcompany.com>  
Subject: athena.cust.com: Configuration Tracking CHANGE  
notification
```

```

Configuration Tracking has detected a CHANGE event
Host: athena.cust.com
Object: /db/file111

```

The email specifies the name of the server and the name of the object that changed. The object can be a file, a directory, or a configuration database.

If you are monitoring a directory target, you receive email about the directory itself and about changes to the files in the directory (except when a file is deleted.) For example, if three new files are created in a directory, you would receive four emails, one for the directory and three for the new files.

If you selected the logging action, an entry is made to the server's standard system log when a change is detected. You select the type of log entry that you want to have written. Opsware SAS uses the following three standard entry types:

- Info
- Warning
- Error

How the entry types are identified is system-dependent. For example, on most systems, Warning entries are identified by the word warning. In some systems, however, a number is used to identify the log entry type.

The following example shows a warning log entry written on a Solaris Server:

```

Jan  8 00:05:25 athena.cust.com Configuration Tracking:
[ID702911
local0.warning] Configuration Tracking: /other/otherfile1 :
Event CHANGE occurred
Jan  8 00:05:25 athena.cust.com Configuration Tracking: [ID
702911
local0.warning] Configuration Tracking: /other/otherfile1 :
Event CHANGE occurred

```

Creating the Email Notification List

Sending email to a server's backup notification list is one of the actions that you can select in a tracking policy entry. The email notification list is a list of email addresses that you define for the following custom attribute:

```

backup_notification_email

```

This attribute can be set on the server itself or on the customer to which the server is attached. Setting the attribute at the customer level allows you to use the same email notification list for all servers that belong to the same customer (assuming that these servers have all been attached to the same customer and do not have the `backup_notification_list` set on the servers themselves). See the *Opware® SAS Policy Setter's Guide* for more information about setting custom attributes for customers.

Search Order for Email Notification List Attribute

On a server that has a policy that includes the Email Notification List for Server action selected, the server searches for the `backup_notification_email` attribute in the following order:

- Server
- Customer

After the custom attribute is found, its value is used (for example, the email address of the notification list) and the search is concluded. If, for example, the `backup_notification_email` attribute is set on a server, the server's email notification list is used, even if the server is assigned to a customer that has a different `backup_notification_email` attribute.

Format of Email Notification List

The notification list can contain multiple email addresses. The email address must be formatted as a comma-separated list.

Customized Configuration Tracking Policies

This section provides information on customizing configuration tracking policies within Opware SAS and contains the following topics:

- Server-Based Entries
- Policies for Customizing Multiple Servers
- Adding or Editing Customized Tracking Policy Entries
- Disabling Customized Tracking Policy Entries
- Enabling Customized Tracking Policy Entries
- Viewing a Server's Tracking Policy
- Reconciling Customized Tracking Policies

- Enabling and Disabling Configuration Tracking on Servers

You can customize the tracking policy for a server or selected group of servers. Ordinarily, a server gets its tracking policy from the policy to which it is attached. In some cases, however, you might need to customize the tracking policy for a particular server or set of servers. If, for example, an application on one server is using an optional configuration file, you can customize the tracking policy for that server so that the optional configuration file is monitored.

Server-Based Entries

A tracking policy entry created for a specific server or selected group of servers is called a server-based tracking policy entry.

Table 13-1 shows the actions that you can perform on server-based tracking policy entries.

Table 13-1: Entry Types

ENTRY TYPE	EDIT	DELETE	ENABLE/DISABLE
Server-based	Yes	Yes	No

To determine if a tracking policy entry server-based, check the Source column in the Track Configurations: Customize Tracking Policies page. Figure 13-1 shows the policy entries for a single selected server.

Figure 13-1: Viewing Configuration Tracking Policy

Return to Managed Servers				
View: Enabled Entries Update				
Add Entry				1 item(s)
<input type="checkbox"/> Target	Type	Action(s)	Source	Common To Total 1 Servers
<input type="checkbox"/> c:\configfiles\config	File Object	Backup, Email Backup Notification List for Server, Log Info	Node	1 Server
Disable		Delete		

Policies for Customizing Multiple Servers

When you customize a tracking policy, you can select one or multiple servers. Here are some considerations when you customize the policies of multiple servers.

- When you select a group of servers that contain both Unix-based (for example, Solaris, HP-UX, Linux, and so forth) and Windows-based servers, you cannot add tracking policy entries. (You can always add entries when you select a single server.)
- When you select a group of servers made up entirely of either Unix-based servers or entirely of Windows-based servers, you have the option of making new tracking policy entries. The policy entries are added to all servers that you select.
- When you select a group of servers made up entirely of either Unix-based servers or of Windows-based servers, you have the option of editing a tracking policy entry. Any policy entry that can be edited can also be added to all selected servers (if it is not already common to all of them).



It can take 20 seconds or longer to customize policies when you select six or more servers.

Adding or Editing Customized Tracking Policy Entries

Use the following procedure to add or edit tracking policy entries for a server or set of servers running the same general type of operating system. If you select a set of servers running both Windows and Unix operating systems, you cannot add tracking policy entries.

- 1 From the navigation panel in the SAS Web Client, click Servers.
- 2 Click **Server Search** to search for the server whose policy you want to edit. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3 Select the server or set of servers that you want to add server-based tracking policy entries to, as Figure 13-2 shows.

Figure 13-2: Selecting Servers

All Statuses All Operating Systems All Stages All Uses All Customers						
All Manufacturers All Models Managed & Deactivated						
Resource Edit View Tasks Configuration Tracking						
<input type="checkbox"/>	Name ^	Host Name / IP Address	OS Version	Stage	Use	Customer
Public Groups						
<input checked="" type="checkbox"/>	core.tr3.opsware.com	core.tr3.opsware.com 172.16.36.18	Red Hat Enterprise Linux AS 3	Not Specified	Not Specified	Opware
<input type="checkbox"/>	m201.tr3.opsware.com	mh03 172.16.36.34	Windows 2000	Not Specified	Not Specified	Not Assigned

- From the Configuration Tracking drop-down menu, select Edit Tracking Policies. The Configuration Tracking: Edit Tracking Policies page appears, as Figure 13-3 shows.

Figure 13-3: Configuration Tracking: Edit Tracking Policies Page

Configuration Tracking: Edit Tracking Policies					
Return to Managed Servers					
View: Enabled Entries Update					
Add Entry					6 item(s)
<input type="checkbox"/> Target	Type	Action(s)	Source	Common To Total 1 Servers	
<input type="checkbox"/> c:\joelongfilename.txt	File Object	Backup, Email, Log Info	Node	1 Server	
<input type="checkbox"/> c:\joeshort.txt	File Object	Backup, Email, Log Warning	Node	1 Server	
<input type="checkbox"/> Com+ Registry Object	Com+ Registry Object	Backup, Log Error	Server	1 Server	
<input type="checkbox"/> HKEY_CLASSES_ROOT\JoeLongKey_09252003	Windows Registry Object	Backup, Email Backup Notification List for Server, Email, Log Warning	Server	1 Server	
<input type="checkbox"/> HKEY_CLASSES_ROOT\JoeShort	Windows Registry Object	Backup, Email Backup Notification List for Server, Email, Log Warning	Server	1 Server	
<input type="checkbox"/> IIS MetaBase Object	IIS MetaBase Object	Backup, Log Warning	Server	1 Server	

Disable **Delete**

- Click **Add Entry** to create a new policy entry. To edit an existing entry, click the link for the entry in the Target field.
- Define the target, select the type, and select the actions to be performed on the target.

Table 13-2 describes each of the selections that you must make.

Table 13-2: Editing Configuration Tracking Policies

FIELD	DESCRIPTION
Type	<p>File: Monitor the file specified in the target field.</p> <p>Directory: Monitor all the files in the directory specified in the target field.</p> <p>The following types are available only for Windows servers:</p> <p>Windows Registry: Specify key in target field.</p> <p>IIS Metabase: Entire Metabase is monitored; do not specify target.</p> <p>COM + Registration Database: Entire Registry is monitored; do not specify target.</p>

Table 13-2: Editing Configuration Tracking Policies (continued)

FIELD	DESCRIPTION
Target	<p>If you selected the file type, specify the full path (including the drive letter on Windows servers) of the file that you want to monitor.</p> <p>If you selected the directory type, specify the full path of the directory (including the drive letter on Windows machines) that you want to monitor. You also have the option of monitoring subdirectories. (Select the include subdirectories check box.)</p> <p>If you select the file or directory type, you can use wildcards in the target. (See the <i>Opware® SAS Policy Setter's Guide</i> for more information about Configuration Tracking Policy Targets and Wildcards.)</p> <p>If you selected the Windows Registry type, specify the Windows registry key. This key and all its subkeys are backed up. Use standard syntax for Windows Registry keys (For example, <code>HKEY_LOCAL_MACHINE\SOFTWARE</code>)</p> <p>If you selected the IIS Metabase or COM + Registration Database type, you do not specify the target.</p>

Table 13-2: Editing Configuration Tracking Policies (continued)

FIELD	DESCRIPTION
Actions (you can select multiple options)	<p>Backup: Back up the specified file, directory, COM + Registration Database, Windows Registry keys, or IIS Metabase.</p> <p>Email Backup Notification List for Server: Send an email to the backup notification list for the selected server. (Not available for Windows Registry.) See “Creating the Email Notification List” on page 467 in this chapter for more information.</p> <p>Email: Send an email to the address or addresses specified in this field when a change is detected. Use a comma-separated list for multiple email addresses. (Not available for Windows Registry.)</p> <p>Log: Add an entry to the server’s system log when a change is detected. (Not available for Windows Registry.)</p> <p>You can choose to write the following types of log entries to the server’s system log:</p> <p>Info</p> <p>Warning</p> <p>Error</p>

- 7** Click **Save** to add the entry to the tracking policy.
- 8** If you want continue to add entries to the tracking policy, click **Add Entry** and repeat this procedure.



Changes do not take effect until you perform a Configuration Tracking policy reconcile.

Disabling Customized Tracking Policy Entries

Perform the following steps to disable customized tracking policy entries:

- 1** From the navigation panel in the SAS Web Client, click Servers.
- 2** Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3** From the Configuration Tracking drop-down menu, select Edit Tracking Policies.

The Configuration Tracking: Edit Tracking Policies page appears.

- 4 Select the tracking policy entry or entries that you want to disable.
- 5 Click **Disable** to disable the tracking policy entries that you selected.



Changes do not take effect until you perform a Configuration Tracking policy reconcile.

Enabling Customized Tracking Policy Entries

Perform the following steps to re-enable tracking policies:

- 1 From the navigation panel in the SAS Web Client, click Servers.
- 2 Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3 From the Configuration Tracking drop-down menu, select Edit Tracking Policies.

The Configuration Tracking: Edit Tracking Policies page appears.

- 4 From the **View** menu, select **Disabled Entries** and then click **Update**.
- 5 Select the tracking policy entry or entries that you want to disable.
- 6 Click **Enable** to disable the tracking policy entries that you select.



Changes do not take effect until you perform a Configuration Tracking policy reconcile.

Viewing a Server's Tracking Policy

Perform the following steps to view a server's tracking policy:

- 1 From the navigation panel in the SAS Web Client, click Servers.
- 2 Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3 From the Configuration Tracking drop-down menu, select Edit Tracking Policies. The tracking policy entries display.
- 4 Click the Tracking Policy link to display the server's tracking policy.

Reconciling Customized Tracking Policies

When you create or edit any customized tracking policy entries, the entries are not deployed to your servers until you perform a configuration tracking reconcile.

A configuration tracking reconcile is not the same as a standard Opsware SAS remediate. Performing a standard remediate does not deploy your tracking policies to your servers.



A configuration tracking reconcile deploys all configuration policies, not just the customized policies.

Perform the following steps to reconcile the tracking policy to the servers whose policies you customized:

- 1** From the navigation panel in the SAS Web Client, click Servers.
- 2** Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3** From the Configuration Tracking drop-down menu, select Reconcile Tracking Policies.

The Track Configurations: Preview Reconcile page appears and displays the progress of the test reconcile.

- 4** After the test reconcile completes successfully, click **Reconcile** to perform the actual reconcile operation.

The Track Configurations: Reconcile page appears.

- 5** If you want to see more information about the changes made during the reconcile operation, click **View Details**. Otherwise, click **Done**.

Enabling and Disabling Configuration Tracking on Servers

You can enable or disable Configuration Tracking on any server or set of servers in your Opsware-managed environment.

Disabling Configuration Tracking is not the same as disabling an individual tracking policy entry (See “Disabling Customized Tracking Policy Entries” on page 473 in this chapter for more information). Disabling Configuration Tracking stops all configuration tracking activity on the selected server.

Disabling configuration tracking, however, does not change a server's tracking policy in any way. If you later re-enabled configuration tracking on the server, the server still has the same tracking policy that it did before you disabled it.

By default, Configuration Tracking is disabled on all managed servers. It is not necessary, however, to manually enable configuration tracking in order to turn on the Configuration Tracking feature. Configuration Tracking is automatically enabled on a server when you reconcile its configuration tracking policies, and you must perform a reconcile in order to deploy tracking policies.



If you want configuration tracking to remain disabled on a server, be careful not to perform a configuration tracking reconcile on the server. (You can, however, still perform a regular reconcile.)

Perform the following steps to enable or disable configuration tracking:

- 1** From the navigation panel in the SAS Web Client, click Servers.
- 2** Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3** Under the Configuration Tracking drop-down menu, select Enable/Disable. A list that displays the state (Enabled/Disabled) of the servers that you selected, as Figure 13-4 shows.

Figure 13-4: Enable/Disable Configuration Tracking Page

[Return to Managed Servers](#)

Enable/Disable Configuration Tracking

Set a server to Enabled or Disabled and click Save.

	Name	Hostname	Stage	Use	Tracking
	M0030.core0.custqa8.com	M0030.core0.custqa8.com	Unknown	Staging	Enabled <input type="button" value="v"/>
	dl360doc	dl360doc	Unknown	UNKNOWN	Enabled <input type="button" value="v"/>
	m094.cust.custqa8.com	m094.cust.custqa8.com	Unknown	UNKNOWN	Enabled <input type="button" value="v"/>
	reports.cust.custqa10.com	reports.cust.custqa10.com	Unknown	Staging	Disabled <input type="button" value="v"/>

- 4 Under the Tracking field, select Enabled or Disabled to enable or disable configuration tracking on the selected server.
- 5 Click **Save** to commit the changes.

Manual Backups

On a server or set of servers, you can perform a manual backup of all tracked configuration files and databases for which you have selected the backup action. Manual backups can be useful as a precaution before making changes to configuration files. If a problem arises, you can then immediately restore a backed-up configuration file or database to its previous state.

Manual backups are full backups. All tracked configuration files and databases for which the backup action has been selected are backed up, not just the files that have changed.

Performing Manual Backups

Perform the following steps to perform a manual backup:

- 1 From the navigation panel in the SAS Web Client, click Servers.
- 2 Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3 From the Configuration Tracking drop-down menu, select Perform Backup Now.
- 4 If you do not want to use the default backup name (Manual Backup), type a new name in the backup name field. If you provide a backup name, you can later perform a search for backup names to find this backup point. Backup names do not have to be unique.
- 5 Click **Start Backup**. The backup progress displays.
- 6 When the backup is completed, you can click **View Details** to review the list of configuration files or configuration databases that have been backed up.

Backup History

Opware SAS provides a detailed history of backup activity as well as search capabilities to find backup points by backup name and to find backed up files by file name. This section contains the following topics:

- Viewing the Backup History
- Viewing the List of Backup Events
- Types of Backup Events
- Backup History Search Options
- Backup Info and Backup Manifest
- File Info and File Versions
- Deleting Backups

Viewing the Backup History

Perform the following steps to view the backup history:

- 1** From the navigation panel in the SAS Web Client, click Servers.
- 2** Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3** From the Configuration Tracking drop-down menu, select View Backup History.

The Track Configurations: View Group Backup History page displays. This page displays the backup activity for the servers that you select. Figure 13-5 shows a sample backup history.

Figure 13-5: Backup History

Configuration Tracking: View Backup History					
Return to Server Search					
View Backup History for a <input type="text" value="Month"/> starting from <input type="text" value="10/18/2003"/> (UTC) matching Backup Name <input type="text"/>					
	10/18/2003	10/25/2003	11/01/2003	11/08/2003	11/15/2003
reports.cust.custqa10.com					
dl360doc	2 Backups				
M0030.core0.custqa8.com	1 Backup				
m094.cust.custqa8.com	21 Backups				

The number of backups that occurred on a particular date displays as a link in the server's date column.

The number of backups refers to the number of backup events (or backup points) when a particular type of backup took place. It does not refer to the number of files backed up. For example, if a server displays 3 backups in a date column, it could refer to the following three backup events:

- A scheduled incremental backup that backed up four files
- A second scheduled incremental backup that backed up 10 files
- A manual backup that backed up 30 files

Viewing the List of Backup Events

To view the list of individual backup events, click the link that displays the number of backups in the desired date column. Figure 13-6 shows a page with a list of backup events.

Figure 13-6: Backup Events

Return to [View Backup History](#)

Properties Network Nodes Install List Installed Packages Custom Attributes Config Tracking History

Backup History Tracking Policy

View by: Backup for a Week starting from 10/18/2003 (UTC) matching Update

<input type="checkbox"/>	Backup Name	Date	User	Type	Files	Size
<input type="checkbox"/>	Manual Backup - 14 servers	10/23/03 UTC	joeadv	Manual Full	14	53.92 KB
<input type="checkbox"/>	Post-RESTORE Backup	10/23/03 UTC	joeadmin	Manual Incremental	8	51.08 KB
<input type="checkbox"/>	Pre-RESTORE Backup	10/23/03 UTC	joeadmin	Manual Incremental	8	43.37 KB
<input type="checkbox"/>	Triggered Backup	10/23/03 UTC	Opsware Agent	Triggered Incremental	5	2.35 KB
<input type="checkbox"/>	Manual Backup	10/23/03 UTC	joeadmin	Manual Full	14	53.92 KB
<input type="checkbox"/>	Post-RESTORE Backup	10/23/03 UTC	joeadmin	Manual Incremental	10	51.39 KB
<input type="checkbox"/>	Pre-RESTORE Backup	10/23/03 UTC	joeadmin	Manual Incremental	1	6.37 KB
<input type="checkbox"/>	Triggered Backup	10/23/03 UTC	Opsware Agent	Triggered Incremental	5	36.9 KB
<input type="checkbox"/>	Manual Backup	10/23/03 UTC	joeadmin	Manual Full	13	53.38 KB
<input type="checkbox"/>	Manual Backup	10/23/03 UTC	joeadmin	Manual Full	11	52.31 KB

Showing 1-10 of 21 | Show All [1 2 3] ▶

Delete Restore selected backups

Types of Backup Events

In addition to information such as the date and time the backup occurred, the list of backup events indicates the type of backup. Table 13-3 describes the type of backup events that can occur.

Table 13-3: Types of Backup Events

TYPE	DESCRIPTION
Triggered Full	The automatic weekly backup of all tracked files for which the backup option was selected. This takes place only if any relevant files have changed since the last full backup.

Table 13-3: Types of Backup Events (continued)

TYPE	DESCRIPTION
Manual Incremental	A backup of all changed files (for which the backup option was selected) that occurs before and after a restoration or a rollback.
Triggered Incremental	An automatic backup that occurs when the Opware Agent detects a change to a tracked file for which the backup option was selected. Only changed files are backed up.
Manual Full	A full backup initiated by the user of all tracked files for which the backup option was selected.

Backup History Search Options

By default, you see the backup history for the past week for the servers that you selected.

If you want to display a different date range, you have the following options:

- Display the backup history for different date range by selecting a different option in the “View Backup History for a” box.
- Use the “starting from” field to search for backup history from a past date until the current date.

You can use the matching field to search for a backup name within the selected date range. Wildcards are allowed (the * and ? characters). If you do not type the full name of the backup, you must use a wildcard for any missing parts of the name.

The results of this search show the date and number of backup names on that date that match the * pattern. When you click the link for the number of backups, a list of the matching backup names displays.

Backup Info and Backup Manifest

When you click a backup name (such as Scheduled Backup) anywhere in the backup history, the Backup Info and Backup Manifest tabs display.

Backup Info Tab

The Backup Info tab displays general information about a backup event. This information includes the name of the backup, the date and time of the backup, and the policies that triggered the backup event.

All customized policies are identified as Server Policy, as Figure 13-7 shows.

Figure 13-7: Track Configurations: View Backup Triggered Backup Page

Track Configurations: View Backup Triggered Backup	
Return to Config Tracking	
Backup Info	Backup Manifest
Name	Triggered Backup
Date	10/23/03 18:09:18
User	Opware Agent
Type	Triggered Incremental
Server	m094.cust.custqa8.com
Policies	Server Policy
Files	5
Size	2.35 KB
Restore	

From the Backup Info tab, you can also place the files that were backed up into the Restore Queue. See “Restoring Backups” on page 488 in this chapter for information about how to use this feature.

Backup Manifest Tab

The Backup Manifest tab displays the list of files that were backed up during the selected backup event, as Figure 13-8 shows.

Figure 13-8: Backup Manifest Tab

Track Configurations: View Backup Triggered Backup							
Return to Config Tracking							
Backup Info	Backup Manifest						
View Files for: All Policies matching <input type="text"/> Update							
<input type="checkbox"/>	File Name	File Type	Size	Modified Date	Policy	Entry Type	Entry Target
<input type="checkbox"/>	c:\curieadir1022	Directory Contents	0 bytes	10/23/03 UTC	Server Policy	Directory Contents	c:\curieadir1022
<input type="checkbox"/>	c:\curieadir1022\New Text Document.txt	File Object	11 bytes	10/23/03 UTC	Server Policy	Directory Contents	c:\curieadir1022
<input type="checkbox"/>	c:\wongtree	Directory Contents	0 bytes	10/23/03 UTC	Server Policy	Directory Tree	c:\wongtree\
<input type="checkbox"/>	c:\wongtree\wongsubtree	Directory Contents	0 bytes	10/23/03 UTC	Server Policy	Directory Tree	c:\wongtree\
<input type="checkbox"/>	c:\wongtree\wongsubtree\New Text Document.txt	File Object	11 bytes	10/23/03 UTC	Server Policy	Directory Tree	c:\wongtree\
Showing 1-5 of 5							
Restore							

Two types of objects are backed up, as seen in the File Type field.

- File Object in the File Type field indicates that a file has been backed up. You can use the entry to restore the file.
- Directory Contents in the File Type field indicates that a directory object has been backed up. The directory object is the directory itself, and not the contents of the directory. You can use this entry to restore the directory, but you must select the files inside the directory to restore the contents of the directory.

The Entry Type field can have three possible values. The Entry Type identifies the target type in the policy entry that caused the file or directory object to be backed up.

- File Object in the Entry Type field indicates that the file was backed up as the result of a file target type.
- Directory Contents in the Entry Type field indicates that the file or directory object was backed up as result of a directory target type.
- Directory Tree in the Entry Type field indicates that the file or directory object was backed up as a result of a directory target type with the include subdirectories option selected.

File Info and File Versions

When you click a file or directory name anywhere in the backup history (such as in the Backup Info tab), the File Info and File Versions tabs display, as Figure 13-9 shows.

Figure 13-9: File Info

Track Configurations: View File c:\curieadir1022\New Text Document.txt	
Return to View Backup	
File Info	File Versions
File Name:	c:\curieadir1022\New Text Document.txt
File Type:	File Object
Size:	11 bytes
Checksum:	08247e49087bad9648a4a8937897b6de
Modified Date:	10/23/03 18:07:58
Backup Date:	10/23/03 18:09:18
Backup Name:	Triggered Backup
Backup Type:	Triggered Incremental
Policy Name:	Server Policy
Entry Type:	Directory Contents
Entry Target:	c:\curieadir1022
Server:	m094.cust.custqa8.com
	<input type="button" value="Restore"/> <input type="button" value="Download"/>

The File Info tab displays information about the specific file that you selected. The Policy Name refers to the policy that caused the file to be backed up. The Policy Name is the Server Policy if the server's customized tracking policy caused the file to be backed up.

You can place the file that you selected in the Restore Queue by clicking Restore. See "Restoration of Backed Up Files" on page 485 in this chapter for more information.

The File Versions tab displays a list of the backed up versions of the file, as Figure 13-10 shows.

Figure 13-10: File Versions

Track Configurations: View File c:\curieadir1022\New Text Document.txt							
Return to View Backup							
File Info		File Versions					
File Name	Size	Checksum	Modified Date	Backup Date ▲	Backup Name	Backup Type	
c:\curieadir1022\New Text Document.txt	11 bytes	08247e49087bad9648a4a8937897b6de	10/23/03 UTC	10/23/03 UTC	Manual Backup - 14 servers	Manual Full	
c:\curieadir1022\New Text Document.txt	11 bytes	08247e49087bad9648a4a8937897b6de	10/23/03 UTC	10/23/03 UTC	Triggered Backup	Triggered Incremental	
c:\curieadir1022\New Text Document.txt	11 bytes	08247e49087bad9648a4a8937897b6de	10/23/03 UTC	10/23/03 UTC	Manual Backup	Manual Full	

Showing 1-3 of 3

It displays the backup name and backup type of the file. If you click any of the files, the File Info for the file is displayed. You can therefore use the File Versions tab to select a different version of the file, and then restore it or download it from the File History.

Deleting Backups

Backups remain in the backup history until you delete them or the server is deactivated. Backups are stored in the Software Repository. You should delete old backup events periodically to reclaim disk storage from the Software Repository.

You can delete entire backup events (identified by a backup name); you cannot delete individual files from the backup history.

See the *Opware® SAS Administration Guide* for more information about mass deletion of backup files.

Perform the following steps to delete backup points from your backup history:

- 1** From the navigation panel in the SAS Web Client, click Servers.
- 2** Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3** Select the server or set of servers that have backup points that you want to delete.
- 4** Search for a date that contains the backup points that you want to delete. Click the link with the number of backup events that occurred on that date.

- 5 Select the check boxes for the backup events that you want to delete from the backup history.
- 6 Click **Delete**.
The Delete Backup Confirmation page appears.
- 7 Click **Delete Backups**. The backups are now deleted.

Restoration of Backed Up Files

You can use the Configuration Tracking feature to restore configuration files or databases that have been backed up. You can restore all files that were backed up during a backup point, or you can select and restore individual files from a backup point. Opsware SAS allows you to rollback a restoration (for example, return your server's tracked files to the state immediately before the restoration).

Overview of Procedures Used to Restore Backed Up Files

This section presents an overview of the procedures you use to restore backed-up configuration files and databases. See “Restoring Backups” on page 488 in this chapter for information about the step-by-step procedure.

To restore backed-up configuration files and databases, view the backup history for a server or set of servers. The backup history displays entries for each date when a backup occurred. As Figure 13-11 shows, the entry for the date displays how many backup points occurred on that date.

Figure 13-11: Backup Points

Configuration Tracking: View Backup History						
Return to Server Search						
View Backup History for a <input type="text" value="Week"/> starting from <input type="text" value="10/23/2003"/> (UTC) matching Backup Name <input type="text"/>						
	10/18/2003	10/19/2003	10/20/2003	10/21/2003	10/22/2003	10/23/2003
reports.cust.custqa10.com						
dl360doc						1 Backup
M0030.core0.custqa8.com						1 Backup
m094.cust.custqa8.com					3 Backups	18 Backups

You select the desired backup date, and you can then select one or more backup points that occurred on that date. Before you restore the backups, you can review all files that were backed up at your selected backup points. You can either choose to restore all backed up files from your selected backup points, or you can select the files individually.

To select the backup, click on the link in the date field that displays the number of backups that were performed on that date.

Restore Queue

This section provides information on the restore queue within Opware SAS and contains the following topics:

- Storing files in the Restore Queue
- Incremental Backups for Restoration and Rollbacks
- Entries for Directories in the Backup History
- File Not Found Entries
- Restoring Backups
- Rolling Back Restored Files

Storing files in the Restore Queue

When you click **Restore**, the files that you selected are placed in the Restore Queue and the View Restore Queue and Perform Restore page appears. You can then review and select files from all the backup points that you selected.

If you do not want to restore the files at this time, you can perform other actions and the files will remain in the Restore Queue as long as your session is active (even if you leave this page). You can also return to the backup history and select other files to put in the Restore Queue.

When you are ready to restore the backups, return to the Track Configurations: Select a Task page and click the **View Restore Queue** and the Perform Restore link.

Incremental Backups for Restoration and Rollbacks

To make rollbacks possible, Opware SAS performs two automatic incremental backups. The first backup occurs immediately before the restoration, and the second occurs immediately after the restoration. Similarly, in order to undo a rollback, Opware SAS performs two automatic incremental backups, one before and one after a rollback.

These backups do not occur if all the files you have selected to restore are identical to the files already on the server. In such a case, the restoration does not in fact change any files on the server, and the rollback option is not available (there are no changes to rollback).

Entries for Directories in the Backup History

As discussed in the “Special Considerations for Directory and Wildcard Targets” in the *Opware® SAS Policy Setter’s Guide*, if you are tracking a directory and the contents of the directory change, the action that you selected is triggered for the directory object itself and for the files that changed. The only exception occurs when a file is deleted from the directory. In that case, the action is triggered for the directory object alone.

If you selected the backup action for the directory target, when the directory contents change, the directory object is backed up as well as the changed files. When a file is deleted, however, only the directory object is backed up.

If you restore files contained in a directory without selecting the entry for the directory object, the directory is re-created on the server if it does not already exist. If you do select the entry for the directory object, however, you can ensure that the directory object is restored with the same properties (such as permissions and time stamp) it had at the selected backup event.

File Not Found Entries

If you are monitoring specific files (as opposed to files monitored in tracked directories and files monitored as the result of wildcard targets), the backup history can contain entries noting “file not found” if the file does not exist on the server, or if the file is later deleted on the server. Similarly, if you are monitoring specific directories (opposed to monitoring directories through wildcard targets), the backup directory can contain “file not found” entries if the directory does not exist on the server, or if the directory is later deleted.

If you select and restore “file not found” entry and the file exists on the server, the file is deleted (it is reverted to the state of the backup event that you selected.)



Exercise caution in restoring entries for deleted directories. If the directory exists on your server and the directory contains files, both the directory and its contents will be deleted.

Restoring Backups

Perform the following steps to restore backed-up configuration files:

- 1** From the navigation panel in the SAS Web Client, click Servers.
- 2** Click **Server Search** to search for the desired servers. (Alternatively, you can click **Manage Servers** and then select the server from the server list.)
- 3** Under the Configuration Tracking drop-down menu, select View Backup History.
- 4** Find the date and server that has the backup points that contain the files that you want to restore. See “Backup History” on page 477 in this chapter for information about finding backup points, viewing backup point details, and viewing lists of backed up files.
- 5** Select the check box for the backup points that have files that you want to restore.
- 6** Click **Restore**.

The files or collection of files from the backup points you selected are placed in the Restore Queue. If you do not want to perform a restore now, you can click the Return to Select a Task link to leave this page. While your session is active, the files remain in the Restore Queue. You can also continue to add more files to the Restore Queue. To return later to the Restore Queue, click the View Restore Queue and Perform Restore from the Track Configurations: Select a Task page.

- 7** If you are ready to restore files, first review the files in the Restore Queue. If you want to restore all the files in the queue, you can select the check box at the top of the list. If you do not want to restore all of the files in the queue, select the checkboxes for the files that you want to restore.
- 8** Click **Restore** (or **Restore All** if you want to restore all of the files in the queue).
- 9** After the restoration is complete, you can click **View Details** for more information about the restored files.

Rolling Back Restored Files

You can rollback any files that you selected to restore. By rolling back the files, you revert the file to the version that was on the server before you performed the restoration. (In other words, you undo the restoration.)

The rollback option is not available if you restored any files that are no longer being monitored by the Configuration Tracking feature. You can choose to restore all changed files or select the files individually.

Perform the following steps to rollback restored files:

- 1** After you restore the backups, click **Rollback**.

The Track Configurations: Restore Queue page appears, which contains the list of files that you need to revert in order to rollback the tracked configuration files to their previous state.

This list might not contain all the files that you selected for your original restore. If any of the files that you selected during your original restore are identical to the files already on the server, they do not need to be rolled back. Only the files that changed display.

- 2** If you want to rollback all the changed files, click **Restore All**. Otherwise, you can select the individual files that you want to rollback and click **Restore**.

The Track Configurations: Restore Progress page appears.



Exercise caution in restoring entries for deleted directories. If the directory exists on your server and the directory contains files, both the directory and its contents will be deleted.

Appendix A: Communication Test Troubleshooting

IN THIS APPENDIX

This section discusses the following topics:

- Overview of Agent Communication Tests
- Command Engine to Agent (AGT)
- Crypto Match (CRP)
- Agent to Command Engine (CE)
- Agent to Data Access Engine (DAE)
- Agent to Software Repository (SWR)
- Machine ID Match (MID)
- Common Troubleshooting Tasks

Overview of Agent Communication Tests

The Communication Test performs the following diagnostic tests to determine if an Agent is reachable:

- **Command Engine to Agent (AGT):** Determines if the Command Engine can communicate with the Agent. The Command Engine is the Opsware SAS component that enables distributed programs to run across many servers. The Command Engine handles the entry of scripts into the Opsware Model Repository (the script storage location in Opsware SAS) and the versioning of stored scripts.
- **Crypto Match (CRP):** Checks that the SSL cryptographic files that the Agent uses are valid.
- **Agent to Command Engine (CE):** Verifies that the Agent can connect to the Command Engine and retrieve a command for execution.

- **Agent to Data Access Engine (DAE):** Checks whether or not the Agent can connect to the Data Access Engine and retrieve its device record. The Data Access Engine provides an XML-RPC interface to the Model Repository that simplifies interaction with various clients such as the SAS Web Client, system data collection, and monitoring agents on servers.
- **Agent to Software Repository (SWR):** Determines if the Agent can establish an SSL connection to the Software Repository. The Software Repository is the central repository for all software that the Opware system technology manages. It contains software packages for operating systems, applications, databases, customer code, and software configuration information.
- **Machine ID Match (MID):** Checks that the Machine ID (MID) on the server matches the MID registered in the Model Repository for the Agent.

When the test run finishes, it returns results that show either success or failure for each test run on each server. For each failed test, the nature of failure is listed by error type in the error details column of the Communication Test window. In some cases, the failure of one test might prevent other tests from being executed.

See "Agent Reachability Communication Tests" on page 125 in Chapter 4 for information about how to run Communication Test.

Command Engine to Agent (AGT)

The Command Engine to Agent (AGT) communications test system checks that the Command Engine can initiate an SSL connection to the Agent and execute an XML/RPC request.

The thirteen possible results are:

- AGT – OK
- AGT – Untested
- AGT – Unexpected error
- AGT – Connection refused
- AGT – Connection time-out
- AGT – Request time-out
- AGT – Server never registered

- AGT – Realm is unreachable
- AGT – Tunnel setup error
- AGT – Gateway denied access
- AGT – Internal Gateway error
- AGT – Gateway could not connect to server
- AGT – Gateway time-out

AGT – OK

No troubleshooting necessary.

AGT – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Command Engine cannot contact the Agent, then no other tests are possible.

What Can I Do If a Test Is Not Run During an AGT Test?

First resolve all tests that failed, and then run the Communication Test again.

AGT – Unexpected error

This result indicates that the test encountered an unexpected error.

What Can I Do If I Get an Unexpected Error?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Opsware, Inc. Customer Support.

AGT – Connection refused

This result indicates that the Command Engine is receiving a TCP reset packet when it attempts to connect to the Agent on port 1002. The likely cause is that the Agent is not running. A firewall might also be blocking the connection.

What Can I Do If the Connection is Refused During an AGT Test?

- 1 Log into the server and confirm that the Agent is running. See “Verifying that an Agent is Running” on page 516 in this appendix for more information.

- 2** If the Agent is not running, restart the Agent. See “Restarting an Opsware Agent” on page 518 in this appendix for more information.
- 3** From the managed server, use netstat to confirm that a socket is in listen mode on port 1002. If not, stop and restart the Agent.
- 4** From the server itself, use Telnet to connect to the IP address of the server where the Agent is installed and port (1002) that the Agent is listening on. If this does not succeed, stop and restart the Agent.
- 5** Verify that the Management IP address that Opsware SAS is using to reach the server is the correct address. See “Checking Management IP of a Managed Server” on page 518 in this appendix for more information. If the IP addresses do not match, stop and restart the Agent, then rerun the test.
- 6** If the previous steps are performed and the test still fails, the problem is likely caused by either a software-based firewall on the server itself or an external firewall blocking the connection.

AGT – Connection time-out

This result indicates that the Command Engine is not receiving any reply packets when it attempts to initiate a TCP connection to the Agent on port 1002. The likely cause is that the server is not running, or that the IP address that Opsware SAS is using to reach the Agent is incorrect. (A firewall might also be blocking the connection.) To check the IP address that Opsware SAS is using to reach the Agent, see “Checking Management IP of a Managed Server” on page 518.

What Can I Do If the Connection Times Out During an AGT Test?

Follow the same steps used to resolve this issue specified in “What Can I Do If the Connection is Refused During an AGT Test?” on page 493.

AGT – Request time-out

This result indicates that the Command Engine is able to successfully complete a TCP connection to the Agent on port 1002, but no response is received from the Agent in response to the XML-RPC request. The likely cause is that the Agent is hung.

What Can I Do If the Request Times Out During an AGT Test?

- 1** Log into the server and restart the Agent. See “Restarting an Opsware Agent” on page 518 in this appendix for more information.

- 2 Check to see whether or not some other process is consistently utilizing an excessive amount of the CPU on the server where the Agent is installed. Also check to see if the system is performing slowly due to a lack of available memory and/or excessive file IO. In any of these cases, the system might be performing too slowly to permit the Agent to respond to the test in a timely manner.

AGT – Server never registered

This test indicates that the server being tested has neither been registered with the Command Engine, nor can it communicate with the Command Engine. The cause of this could be any number of reasons similar to those in the Agent to Command Engine (CE) test. It is also possible (but unlikely) that the Agent was installed but never started.

What Can I Do If the Server Has Not Been Registered with the Command Engine During an AGT Test?

To troubleshoot this error, use the following procedures:

- 1 Ensure that the Agent is running. For these instructions, See “Verifying that an Agent is Running” on page 516 in this appendix for more information.
- 2 Ensure that the Agent can contact the Command Engine.
- 3 If the Agent is in a Satellite facility, ensure that its Gateways are properly configured and that it is properly configured to use those Gateways. See “Checking Network Gateway Configuration” on page 518 in this appendix for more information.
- 4 If the Agent is not in a Satellite:
 - Ensure the host name “way” (no quotes) resolves to its valid IP address. See “Resolving Host Name” on page 519 in this appendix for more information.
 - Verify that a connection can be established to port 1018 of way. Use the command “telnet way 1018” (or equivalent).

One (or more) of the above checks will fail. To solve that failure, refer to the corresponding error code for the Agent to Command Engine (CE) test on page 499, or to the realm connectivity and configuration test.

AGT – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This means that a path of tunnels between the Gateways in the Opsware core and the realm of the managed server cannot be established.

What Can I Do If the Realm Is Unreachable During an AGT Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact Opsware, Inc. Customer Support for assistance in troubleshooting the Gateway network.

AGT – Tunnel setup error

The Command Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What Can I Do If I Get a Tunnel Setup Error During an AGT Test?

Contact your Opsware administrator.

AGT – Gateway denied access

The Gateway is working but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Command Engine access to the Agent.

What Can I Do If the Gateway is Denied Access During an AGT Test?

Contact your Opsware administrator.

AGT – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do If There is an Internal Gateway Error During an AGT Test?

Contact your Opsware administrator.

AGT – Gateway could not connect to server

The Gateway could not establish a connection to the Agent. This might be because the Agent is not running, or because a firewall might be blocking the connection.

What Can I Do If the Gateway Couldn't Connect to the Server During an AGT Test?

If you suspect the Agent is not running, see “Verifying that an Agent is Running” on page 516. To make sure that the Gateway can establish a connection to the IP address of the server where the Agent is installed, try to ping the IP address of the server where the Agent is installed.

AGT – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do If the Gateway Times Out During an AGT Test

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the Opsware core.

Crypto Match (CRP)

This test checks that the SSL cryptographic files that the Agent uses are valid.

The five possible results are:

- CRP – OK
- CRP – Untested
- CRP – Unexpected error
- CRP – Agent certificate mismatch
- CRP – SSL negotiation failure

CRP – OK

No troubleshooting necessary.

CRP – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot be reached, then no other tests are possible.

What Can I Do If a Test Is Not Run During a CRP Test?

First resolve all tests that failed, and then run the Communication Test again.

CRP – Unexpected error

This result indicates that the test encountered an unexpected error.

What Can I Do If I Get an Unexpected Error During a CRP Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Opware, Inc. Customer Support.

CRP – Agent certificate mismatch

This result indicates that the SSL certificate that the Agent is using (cogbot.srv) does not match the SSL certificate that is registered with Opware SAS for that Agent.

What Can I Do If I Get a Certificate CN Mismatch During a CRP Test?

Use the Recert Agent Custom Extension to issue a new certificate to the Agent. See “Opware SAS Custom Extensions” on page 428 in Chapter 11 for more information.

CRP – SSL negotiation failure

This result indicates that the Agent is not accepting SSL connections for the Opware core. (The Opware core is the entire collection of servers and services that provide Opware SAS services.) The likely cause of this error is that one or more files in the Agent crypto directory are missing or are invalid.

What Can I Do If I Get an SSL Negotiation Failure During an CRP Test?

Run the Server Recert custom extension in the “set allow recert flag only” mode on the server, and then Run the Opware Agent Installer with the “-c” switch.

Reinstalling the Agent with the “-c” option (“c” stands for “clean”) removes all certs on the server and also removes the MID file, which forces the Agent to retrieve a new MID from the Data Access Engine.

- See “Opware SAS Custom Extensions” on page 428 in Chapter 11 for more information how to run the Recert Agent Custom Extension to issue a new certificate to the Agent.
- See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for information about how to install an Opware Agent using the “-c” switch.

After you reinstall the Agent, run the test again to check if the Agent is now reachable.

Agent to Command Engine (CE)

This test checks that the Agent can connect to the Command Engine and retrieve a command for execution.

The sixteen possible results are:

- CE – OK
- CE – Untested
- CE – Unexpected error
- CE – Connection refused
- CE – Connection time-out
- CE – DNS does not resolve
- CE – Old Agent version
- CE – Realm is unreachable
- CE – No Gateway defined
- CE – Tunnel setup error
- CE – Gateway denied access
- CE – Gateway name resolution error
- CE – Internal Gateway error
- CE – Gateway could not connect to server
- CE – Gateway time-out
- CE – No callback from Agent

CE – OK

No troubleshooting necessary.

CE – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Command Engine, then no other tests are possible.

What Can I Do If a Test Is Not Run During a CE Test?

First resolve all tests that failed, and then run the Communication Test again.

CE – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During a CE Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Opsware, Inc. Customer Support.

CE – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Command Engine on port 1018. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Command Engine. It is also possible that a firewall might be blocking the connection.

What Can I Do If the Connection is Refused During a CE Test?

- 1** Check that the name “way” resolves to its correct IP address. For instructions on how to do this, see “Resolving Host Name” on page 519.
- 2** Check to make sure there isn't a firewall refusing the connection to this IP address.

CE – Connection time-out

This result indicates that the Agent is not receiving any reply packets when it attempts to initiate a TCP connection to the Command Engine on port 1018. The likely cause is that the Agent is connecting to the “wrong” IP address. In other words, the Agent doesn't know the correct IP address of the Command Engine. A firewall might also be blocking the connection.

What Can I Do If the Connection Times Out During a CE Test?

Follow the same steps specified in What Can I Do If the Connection is Refused During a CE Test?.

CE – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “way” to a valid IP address. In other words, the Agent does not know the correct IP address of the Command Engine.

What Can I Do If the Command Engine Name Does Not Resolve During a CE Test?

Log into the server and use a command such as Telnet to confirm that the host name “way” can resolve (for example: “telnet way 1018”). If not, check the DNS configuration of the server to make sure that the host name “way” is configured to its correct IP address. See “Resolving Host Name” on page 519 in this appendix for more information.

CE – Old Agent version

This result indicates that the Agent was unable to contact the Command Engine, but the test was unable to determine the exact cause because the Agent is out of date.

What Can I Do If the Agent is Out of Date During a CE Test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Command Engine (“way”) did not resolve, or the connection was refused.

- If you believe that the host name of the Command Engine (“way”) did not resolve, then See “CE – DNS does not resolve” on page 501 in this appendix for more information.
- If you determine that the connection was refused, See “CE – Connection refused” on page 500 in this appendix for more information.

Alternatively, you can upgrade the Agent to the latest version (contact Opsware, Inc. Customer Support) and re-run the test. See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for information about how to install an Agent.

CE – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the Gateways in the Opsware core and the realm of the managed server cannot be established.

What Can I Do if the Realm is Unreachable During a CE Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your Opsware administrator for assistance in troubleshooting the Gateway network.

CE – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What Can I Do If No Gateway is Defined During a CE Test?

To troubleshoot this error, try the following:

- 1** Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:

- **Unix/Linux:** /var/lc/cogbot/etc
- **Windows:** %SystemDrive%\Program Files\Common Files\Loudcloud\cogbot\etc

- 2** Make sure that this file contains a single line as shown:

```
opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_
address>:<gw_port>
```

CE – Tunnel setup error

The Command Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What Can I Do If A Tunnel Setup Occurs Error During a CE Test?

Contact your Opsware administrator.

CE – Gateway denied access

The Gateway is working, but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Command Engine.

What Can I Do if the Gateway is Denied Access During a CE Test?

Contact your Opsware administrator.

CE – Gateway name resolution error

The server running the Gateway in the Opsware core was unable to resolve the host name "way". It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What Can I Do if a Name Resolution Error Occurs on the Gateway During a CE Test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “way” can be resolved (for example: “host way”).

If you cannot connect, contact your Opsware administrator so that you can check the DNS configuration of the core Gateway server.

CE – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do if an Internal Gateway Error Occurs During a CE Test?

Contact your Opsware administrator.

CE – Gateway could not connect to server

The Gateway could not establish a connection to the Command Engine. The situation might be because the Command Engine is not running, or because the Gateway is resolving the Command Engine host name (“way”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What Can I Do if the Gateway Can't Connect to Server During a CE Test?

Check that the name “way” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP. See “Resolving Host Name” on page 519 and “Verifying that a Port is Open on a Managed Server” on page 517 in this appendix.

CE – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do if the Gateway Times Out During a CE Test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the Opsware core.

CE – No callback from Agent

The Command Engine was able to contact the Agent, but the Agent did not call back to retrieve its command. However, the Agent reports that it can connect to a Command Engine. This most likely means that the managed server's name resolution mechanism (such as DNS) is not configured to point the server to a different Opware core facility than is currently stored for the server by Opware SAS.

What Can I Do if There is No Callback from Agent?

It is possible that the MID file is missing. If the MID file is missing, it can be recreated easily by creating a file called 'mid' in the correct location which contains the value of the "Server ID" from the Server's Properties page in the SAS Web Client.

If the MID file is not missing, then ensure that the server's name resolution mechanism (DNS, NIS, and so on) is properly configured so that the host names "spin" and "way" resolve to the appropriate IP addresses or Opware core services in the same core, and that those hosts can be reached from the server on ports 1004 and 1018, respectively. If this is the case, it is likely that the server has been redirected to a different core recently, and the Agent has not yet registered, which will cause Opware SAS to update its records. If this issue remains unresolved for more than 12 hours, contact Opware, Inc. Customer Support.

Agent to Data Access Engine (DAE)

This test checks that the Agent can retrieve its device record from Data Access Engine. The fifteen possible results are:

- DAE – OK
- DAE – Untested
- DAE – Unexpected error
- DAE – Connection refused
- DAE – Connection time-out
- DAE – DNS does not resolve
- DAE – Old Agent version
- DAE – Realm is unreachable
- DAE – No Gateway defined
- DAE – Tunnel setup error

- DAE – Gateway denied access
- DAE – Gateway name resolution error
- DAE – Internal Gateway error
- DAE – Gateway could not connect to server
- DAE – Gateway time-out

DAE – OK

No troubleshooting necessary.

DAE – Untested

This result is returned when a functional area cannot be tested, because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Data Access Engine then no other tests are possible.

What Can I Do If a Test Is Not Run During a DAE Test?

First resolve all tests that failed, and then run the Communication Test again.

DAE – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During a DAE Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Opsware, Inc. Customer Support.

DAE – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Data Access Engine on port 1004. The likely cause is that the Agent is connecting to the wrong IP address. A firewall might also be blocking the connection.

What Can I Do If the Connection is Refused During a DAE Test?

- 1** Check that the name “spin” resolves to its correct IP address. See “Resolving Host Name” on page 519 in this appendix for more information.
- 2** Check to make sure that a firewall is not refusing the connection to this IP address.

DAE – Connection time-out

This result indicates that the Agent is not receiving any reply packets when it attempts to initiate a TCP connection to the Data Access Engine on port 1004. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Command Engine. A firewall might also be blocking the connection.

What Can I Do If the Connection Times Out During a DAE Test?

Follow the same steps specified in “What Can I Do If the Connection is Refused During a DAE Test?” on page 505.

DAE – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “spin” to a valid IP address. In other words, the Agent does not know the correct IP address of the Data Access Engine.

What Can I Do If the Data Access Engine Name Does Not Resolve During a DAE Test?

Log into the server and use a command such as Telnet to confirm that the host name “spin” can be resolved (for example: telnet spin 1004”). If not, check the DNS configuration of the server to make sure that the host name “spin” is configured to its correct IP address. See “Resolving Host Name” on page 519 in this appendix for more information.

DAE – Old Agent version

This result indicates that the Agent was unable to contact the Data Access Engine, and the test is unable to determine the exact cause, because the Agent is out of date.

What Can I Do If the Agent is Out of Date During an DAE Test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Data Access Engine (“spin”) did not resolve, or the connection was refused.

- If you believe that the host name of the Data Access Engine (“way”) did not resolve, then see “DAE – DNS does not resolve” on page 506.
- If you determine that the connection was refused, see “DAE – Connection refused” on page 505.

Alternatively, you can upgrade the Agent to the latest version (contact Opsware, Inc. Customer Support) and re-run the test. See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for information about how to install an Agent.

DAE – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the gateways in the Opsware core and the realm of the managed server cannot be established.

What Can I Do if the Realm is Unreachable During a DAE Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your Opsware administrator for assistance in troubleshooting the Gateway network

DAE – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What Can I Do If No Gateway is Defined During a DAE Test?

To troubleshoot this error, try the following:

- 1** Create or open the `opswgw.args` file on the managed server. The `opswgw.args` file is located on the managed server at:
 - **Unix/Linux:** `/var/lc/cogbot/etc`
 - **Windows:** `%SystemDrive%\Program Files\Common Files\Loudcloud\cogbot\etc`

- 2** Make sure this file contains a single line as shown:

```
opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_
address>:<gw_port>
```

DAE – Tunnel setup error

The Data Access Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What Can I Do if a Tunnel Setup Error Occurs During a DAE Test?

Contact your Opsware administrator.

DAE – Gateway denied access

The Gateway is working, but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Data Access Engine.

What Can I Do if the Gateway is Denied Access During a DAE Test?

Contact your Opware administrator.

DAE – Gateway name resolution error

The server running the Gateway in the Opware core was unable to resolve the host name "spin". It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What Can I Do if There is a Name Resolution Error on the Gateway During a DAE Test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name "spin" can be resolved (for example: "host spin").

If you cannot connect, contact your Opware administrator so that you can check the DNS configuration of the core Gateway server.

DAE – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do if an Internal Gateway Error Occurs During a DAE Test?

Contact your Opware administrator.

DAE – Gateway could not connect to server

The Gateway could not establish a connection to the Data Access Engine. This might be because the Data Access Engine is not running, or because the Gateway is resolving the Data Access Engine host name ("spin") to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What Can I Do if the Gateway Can't Connect to Server During a DAE Test?

Check that the name "spin" resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP. See "Resolving Host Name" on page 519 in this appendix for more information and See "Verifying that a Port is Open on a Managed Server" on page 517 in this appendix for more information.

DAE – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do if the Gateway Times Out During a DAE Test?

Ensure that network connectivity is available between the Gateways in the path between the managed server's realm and the Opsware core.

Agent to Software Repository (SWR)

This test checks that the Agent can establish an SSL connection to the Software Repository.

There 16 possible results are:

- SWR – OK
- SWR – Untested
- SWR – Unexpected error
- SWR – Connection refused
- SWR – Connection time-out
- SWR – DNS does not resolve
- SWR – Old Agent version
- SWR - Server identification error
- SWR – Realm is unreachable
- SWR – No Gateway defined
- SWR – Tunnel setup error
- SWR – Gateway denied access

- SWR – Gateway name resolution error
- SWR – Internal Gateway error
- SWR – Gateway Could not connect to server
- SWR – Gateway time-out

SWR – OK

No troubleshooting necessary.

SWR – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Software Repository, then no other tests are possible.

What Can I Do If a Test Is Not Run During a SWR Test?

First resolve all tests that failed, and then run the Communication Test again.

SWR – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During a SWR Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Opsware, Inc. Customer Customer Support.

SWR – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Software Repository on port 1003. The likely cause is that the Agent is trying to connect to the wrong IP address. A firewall might also be blocking the connection.

What Can I Do If the Connection is Refused During an SWR Test?

- 1** Check that the name “theword” resolves to the correct IP address. For this information, see “Resolving Host Name” on page 519.
- 2** Check to make sure that a firewall isn’t refusing the connection to this IP address.

SWR – Connection time-out

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Software Repository on port 1003. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Software Repository. A firewall might also be blocking the connection.

What Can I Do If the Connection Times Out During an SWR Test?

Follow the same steps specified in “What Can I Do If the Connection is Refused During an SWR Test?” on page 510.

SWR – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “theword” to a valid IP address. In other words, the Agent does not know the correct IP address of the Software Repository.

What Can I Do If the Software Repository Name (“theword”) Does Not Resolve During an SWR Test?

Log into the server and use a command such as Telnet to confirm that the host name “theword” can be resolved (for example: “telnet theword 1003”). If not, contact your Opsware administrator so that you can check the DNS configuration of the server.

SWR – Old Agent version

This result indicates that the Agent was unable to contact the Software Repository, and the test is unable to determine the exact cause because the Agent is out of date.

What Can I Do If the Agent is Out of Date During an SWR Test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Software Repository (“theword”) did not resolve, or the connection was refused.

- If you think that the host name of the Software Repository (“theword”) did not resolve, then see “SWR – DNS does not resolve” on page 511.
- If you determine that the connection was refused, see “SWR – Connection refused” on page 510.

Alternatively, you can upgrade the Agent to the latest version (contact Opsware, Inc. Customer Support) and re-run the test. See “Opsware Agent Installation Using ODAD” on page 115 in Chapter 4 for information about how to install an Opsware Agent.

SWR - Server identification error

Whenever an Agent makes a request of the Software Repository, the identity of the server is validated to confirm that the server should be allowed access to the information requested. This error indicates that the Software Repository was unable to identify the server being tested, or incorrectly identified that server.

What Can I Do If I Get a Server Identification Error?

The Software Repository identifies servers based on the incoming IP address of the request. To troubleshoot this error, try the following:

- 1** Check the Device Properties tab for the server in the SAS Web Client to see if Network Address Translation (NAT) is in use. If it is, make sure that NAT is statically configured, and that only one server is using the NAT address. If multiple servers are using the same IP address, you will need to reconfigure the NAT device. See “Network Address Translation (NAT) for Managed Servers” on page 275 in Chapter 8 for more information.
- 2** If the Agent is installed on a cluster, check that each node in the cluster has a unique IP address at which it can be reached. You might have to add static routes to the server to ensure that connections made from that server to the Opware core use the unique IP. If NAT is not in use, you can alternately mark the correct interface as the “primary” interface through the Network Configuration tab for the server in the SAS Web Client. See “Network Address Translation (NAT) for Managed Servers” on page 275 in Chapter 8 for more information.
- 3** The server's IP address might have changed recently. If this is the case, stop and restart the Agent. For instructions on how to stop and start an Agent, see “Restarting an Opware Agent” on page 518.

SWR – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the gateways in the Opware core and the realm of the managed server cannot be established.

What Can I Do if the Realm is Unreachable During a SWR Test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your Opware administrator for assistance in troubleshooting the Gateway network.

SWR – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What Can I Do If No Gateway is Defined During a SWR Test?

To troubleshoot this error, try the following:

- 1** Create or open the `opswgw.args` file on the managed server. The `opswgw.args` file is located on the managed server at:

- **Unix/Linux:** `/var/lc/cogbot/etc`
- **Windows:** `%SystemDrive%\Program Files\Common Files\Loudcloud\cogbot\etc`

- 2** Make sure that this file contains a single line as shown:

```
opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_
address>:<gw_port>
```

SWR – Tunnel setup error

The Data Access Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What Can I Do If a Tunnel Setup Error Occurs During a SWR Test?

Contact your Opsware administrator.

SWR – Gateway denied access

The Gateway is working but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Software Repository.

What Can I Do if the Gateway is Denied Access During a SWR Test?

Contact your Opsware administrator.

SWR – Gateway name resolution error

The server running the Gateway in the Opsware core was unable to resolve the host name "theword". It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What Can I Do if a Name Resolution Error Occurs on the Gateway During a SWR Test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “theword” can be resolved (for example: “host theword”).

If you cannot connect, contact your Opsware administrator so that you can check the DNS configuration of the core Gateway server.

SWR – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What Can I Do if an Internal Gateway Error Occurs During a SWR Test?

Contact your Opsware administrator.

SWR – Gateway Could not connect to server

The Gateway couldn't establish a connection to the Software Repository. This error might be because the Software Repository is not running, or because the Gateway is resolving the Software Repository host name (“theword”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What Can I Do if the Gateway Can't Connect to Server During a SWR Test?

Check that the name “theword” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP address. For more information, see “Resolving Host Name” on page 519 and “Verifying that a Port is Open on a Managed Server” on page 517.

SWR – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What Can I Do if the Gateway Times Out During a SWR Test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the Opsware core.

Machine ID Match (MID)

This test checks whether the MID that the Agent reported matches that recorded in the Model Repository (Opsware data repository).

You can receive four possible errors from the Machine ID (MID) Communication Test:

- MID – OK
- MID – Untested
- MID – Unexpected error
- MID – MID mismatch

MID – OK

No troubleshooting necessary.

MID – Untested

This result is returned when a functional area cannot be tested, because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Model Repository, then no other tests are possible.

What Can I Do If a Test Is Not Run During an MID Test?

First resolve all tests that failed, and then run the Communication Test again.

MID – Unexpected error

This result indicates that the test encountered an unexpected condition.

What Can I Do If I Get an Unexpected Error During an MID Test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Opsware, Inc. Customer Support.

MID – MID mismatch

This result indicates that the MID that the Agent reported does not match the recorded MID in the Model Repository for that Agent. The likely cause is that the Command Engine is running the test against the wrong Agent.

What Can I Do If the MID is Mismatched During an MID Test?

To troubleshoot this error, try the following:

- 1** Check the Device Properties tab for the server in the SAS Web Client to see if NAT is in use for this server. If it is, make sure that static, 1-to-1 NAT is being used. Opsware SAS requires that all managed servers be reachable on a distinct, consistent IP address, so configurations that assign addresses dynamically or use port-based translation are not supported.
- 2** If the Agent is installed on a cluster, check that each node in the cluster has a unique IP address at which it can be reached. You might have to add static routes to the server to ensure that connections made from that server to the Opsware core use the unique IP. If NAT is not in use, you can alternately mark the correct interface as the "primary" interface via the Network Configuration tab for the server in the SAS Web Client.
- 3** The IP address might have changed recently. If this is the case, stop and restart the Agent. For these instructions, see "Restarting an Opsware Agent" on page 518.

Common Troubleshooting Tasks

The following list of troubleshooting tasks are common to more than one Communication Test error:

- Verifying that an Agent is Running
- Verifying that a Port is Open on a Managed Server
- Restarting an Opsware Agent
- Checking Management IP of a Managed Server
- Checking Network Gateway Configuration
- Resolving Host Name

Verifying that an Agent is Running

To verify that an Agent is running on a server, perform the following steps:

- 1** On Solaris, HP-UX, or AIX, enter this argument at the command line:

```
/usr/ucb/ps auxwww | grep cog
```

You should get this result if the Agent is running:

```
/opt/OPSW/bin/python /opt/OPSW/blackshadow/shadowbot/
daemonbot.pyc --conf /var/lc/cogbot/etc/cogbot.args
```

- 2** On Linux, enter this argument at the command line:

```
ps auxwww | grep cog
```

You should get this result if the Agent is running:

```
/opt/OPSW/bin/python /opt/OPSW/blackshadow/shadowbot/
daemonbot.pyc --conf /var/lc/cogbot/etc/cogbot.args
```

- 3** On Windows, from the Administrative Tools | Services, check to make sure that the 'shadowbot' service is running.

Verifying that a Port is Open on a Managed Server

For some errors, you will need to verify that the port is open on the server where the Agent is installed. To do this, perform the following steps:

- 1** Check if the port is open.
- 2** On Solaris, HP-UX, AIX, or Linux enter:

```
netstat -an | grep 1002 | grep LISTEN
```

If the port is open on the box, you should get back the following:

```
*.1002    *.*      0        0 24576    0 LISTEN
```

- 3** On Windows, at the command prompt enter:

```
netstat -an | find "1002" | find "LISTEN"
```

If the port is open on the box, you should get back the following result:

```
TCP0.0.0.0:10020.0.0.0:0LISTENING
```

- 4** Confirm that the port is actually open. To do this, from the computer where the Agent is installed, Telnet to port 1002 by using both localhost and the external IP address of the server. Performing the Telnet will help you confirm that a connection refused message is being caused by the lack of an open port on the managed server rather than a problem with networking hardware between the core and the managed server.

Restarting an Opware Agent

For Solaris, Linux, or AIX, perform the following steps:

- 1 To stop an Opware Agent on Solaris, Linux, or AIX, execute the following command:

```
/etc/init.d/cogbot stop
```

- 2 To restart the Opware Agent on Solaris, Linux, or AIX, execute the following command:

```
/etc/init.d/cogbot start
```

For HP-UX, perform the following steps:

- 1 To stop an Opware Agent on HP-UX, execute the following command:

```
/sbin/init.d/cogbot stop
```

- 2 To restart an Opware Agent on HP-UX, execute the following command:

```
/sbin/init.d/cogbot start
```

For Windows, execute the following command to stop and start an Opware Agent:

```
net stop shadowbot  
net start shadowbot
```

Checking Management IP of a Managed Server

To check the Management IP of a managed server, perform the following steps:

- 1 To view the management IP of the managed server, log into the SAS Web Client.
- 2 From the Navigation panel, click Servers ► Manage Servers.
- 3 From the Manage Servers list, click the display name of the server for which you want to check the Management IP.
- 4 Select the Network tab of the server's properties.
- 5 Check to make sure that the Management IP address matches the IP address of the managed server.

Checking Network Gateway Configuration

To check the network Gateway configuration, perform the following steps:

- 1 On Solaris, enter this command to check routing table:

```
netstat -rn
```

Your results should look like this:

```
default          192.168.8.1      UG          1    5904
```

where 192.168.8.1 is the IP of the Gateway.

- 2** On Linux, enter this command to check routing table:

```
route -n
```

Your results should look like this:

```
0.0.0.0          192.168.8.1     0.0.0.0      UG    0    0
0 eth0
```

where 192.168.8.1 is the IP of the Gateway.

- 3** On Windows, enter this command to check routing table:

```
route print
```

Your results should look something like this:

```
0.0.0.00.0.0.0192.168.8.1192.168.8.12020
```

where 192.168.8.1 is the IP of the Gateway.

- 4** In each case, you should also ping 192.168.8.1 (IP) to confirm that you can actually reach the Gateway.

Resolving Host Name

All managed servers (those with agents) must be able to resolve unqualified Opsware SAS service names for the following components:

- spin (Data Access Engine)
- way (Command Engine)
- theword (Software Repository)

If you need to ensure that one of these host names resolves correctly, contact your Opsware administrator to find out what qualified host name or IP address these service names should resolve to.

- 1** Try to ping the host. For example, execute the following command if you wanted to resolve the host name, way:

```
ping way
```

- 2** If the host name cannot resolve, you will get the following errors:

Linux/Solaris/AIX/HP-UX:

```
ping: unknown host way
```

Windows:

```
Ping request could not find host way. Please check the name  
and try again.
```

- 3** If the host name can resolve, you might get back various permutations of these types of messages (OS independent):

```
way is alive
```

or

```
pinging way (ip) with 32 bytes of data
```


Appendix B: Opsware Agent Utilities

IN THIS APPENDIX

This section discusses the following topics:

- Agent Installation Using the CLI
- Opsware Agent Upgrade Tool
- Opsware Agent Upgrade Custom Extension

Agent Installation Using the CLI

This section provides information on Opsware Agent installation using the Agent Installer CLI and contains the following topics:

- Overview of Agent Installation Using the CLI
- Preparation for Opsware Agent Installation
- Preassimilation Checklist
- Installing an Opsware Agent by using the Agent Installer CLI
- Opsware Agent Installer Options
- Example: Opsware Agent Installer Command and Options
- Starting an Opsware Agent on a Server
- Verifying Opsware Agent Functionality
- Augmenting the Information for a Managed Server
- Uninstalling an Opsware Agent on Unix and Windows
- Uninstalling Earlier Versions of Opsware Agents on Unix
- Uninstalling Earlier Versions of Opsware Agents on Windows

Overview of Agent Installation Using the CLI



When you install Opsware Agents on existing operational servers, you should synchronize the local time on the servers with an external time-server that uses a network time protocol (NTP).

Installing Opsware Agents on servers makes existing operational servers known to Opsware SAS so that they can be managed. Assimilating servers into Opsware SAS is appropriate when many servers are already functioning in the operational environment and need to be managed (for example, when Opsware technology is initially deployed in a facility).

Installing an Opsware Agent on a server with a pre-built OS into Opsware SAS enables:

- Baseline discovery of the operating system on the server.
- Managing the baseline operating system, including patch management, when the operating system is defined in Opsware SAS with the Prepare Operating System Wizard.
- Full provisioning and management capabilities for any new applications deployed on the server.

When installed, the Opsware Agent registers the server with the Opsware Model Repository. Opsware SAS assigns the server to a generic operating system that corresponds to the operating system that the Opsware Agent discovered during the installation. The server is assigned to a placeholder OS node. For each operating system, the SAS Web Client contains a node `<operating_system_version>/Not Assigned`.

The Opsware Agent Installer can install Agents when an Opsware core is not available to a server. If a newly-installed Agent cannot contact a core, the Agent runs in a dormant mode. While dormant, it periodically attempts to contact the core. When the core becomes available, the Agent performs the initialization tasks, such as hardware and software registration, that usually take place when the Agent is first installed.

The server is tracked in the SAS Web Client. However, the server operating system *cannot* be managed while the server is assigned to the generic operating system node. You must reassign the server to the operating system that was defined with the OS Provisioning feature.

The server is associated with the default facility for the local instance of Opware SAS.

If the managed server's IP address does not fall within a specified IP range, the server is associated with the default IP range group (Default). The default group is associated with the customer Not Assigned.

See the *Opware[®] SAS Policy Setter's Guide* for information about how servers are associated with customers.

Users install an Opware Agent on each server. Running an Opware Agent on a server allows Opware SAS to manage the server. To install an Opware Agent, run the Opware Agent Installer.

The Opware Agent Installer is an application that has the following features:

- Can be invoked from the command line or within a script.
- Installs an Opware Agent.
- Logs its decisions and actions.
- Can be operated unattended because user interaction is not required.

The Opware Agent Installer installs the Opware Agent, retrieves cryptographic material, retrieves configuration information, and writes a configuration file.

Preparation for Opware Agent Installation

Opware Inc. recommends that you set up a Windows file share to make the Opware Agent Installer for various operating systems available from one place. Setting up a file share allows you to install Opware Agents on servers quickly and easily. If this is not possible, the Opware Agent Installer needs to be moved by using an alternate file transfer mechanism, such as SFTP.

At the completion of the Opware Agent installation process, a managed server is assimilated and the hardware and software data that the Opware Agent discovered is stored in the Model Repository.



To use the Patch Management features on Windows NT 4.0 and Windows 2000 servers, you must install Internet Explorer (IE) 6.0 or later on the server first because a patch utility depends on it. If you do not install IE 6.0 on the server first, the Opware Agent Installer warns you that the Patch Management feature does not work as expected because it checks for IE 6.0 on all Windows servers. This prerequisite is not required for Windows 2003, because IE 6.0 is pre-installed for this operating system.

Preassimilation Checklist

Prior to installation, you should perform the following tasks on the server where the Opware Agent is to be installed. Performing these tasks is vital to installing the Opware Agent quickly within maintenance windows.

- 1** For the Code Deployment & Rollback feature, verify that the following port is accessible between the server you will push code from and the server where you will push code to:

- `telnet <staging_server> 1002`
- `telnet <production_server> 1002`

- 2** Because the Opware Agent runs on port 1002, verify that no other applications are using this port.

- On a Unix server, enter this command from a terminal window:

```
netstat -an | grep 1002 | grep LISTEN
```

- On a Windows server, enter this command from a terminal window:

```
netstat -an | find "1002" | find "LISTEN"
```

- 3** Check for sufficient disk space for Opware Agent installation on the server.

The Opware Installer checks for the following amounts of free disk space in these directories:

- 30MB in `/opt/OPSW/installdir` (Unix)
- 100MB in `/var/lc/var_dir` (Unix)
- 30MB in `%SystemDrive%\Program Files\Loudcloud\installdir` (Windows)
- 100MB in `%SystemDrive%\Program Files\Common Files\Loudcloud\var_dir` (Windows)

(These default directories can be overridden with parameters at installation time.)

These space requirements might not be enough. The `vardir` directory is used for dynamic content like logs and downloaded packages. If there is not enough disk space for the packages during remediation, it will fail.

4 On the Solaris operating system, check for legacy sun4m architecture. Currently, the Opsware Agent works only for sun4u architecture.

5 For Windows, check the following items:

– At a minimum, NT 4.0 Service Pack 6a must be installed on the server.

– Verify that the Windows Registry has the correct settings:

1. Start `regedit` and locate the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\FileSystem
```

2. Select the `NtfsDisable8dot3NameCreation` entry.

3. On the **Edit** menu, click **DWORD** and verify that the value is set to 0. The value *must* be set to 0. If necessary (because the value is set to 1), change the value by following your organization's IT policies and reboot the server.

6 To install an Opsware Agent on a server running Solaris, you must also install the following Solaris packages:

For Python:

```
SUNWtoo
SUNWtoox
```

For showrev:

```
SUNWadm
SUNWlibC
SUNWlibCx
SUNWadmfw
```

- 7** Before you install an Agent on a server, the server must meet certain package and patch requirements that vary by operating system, as Table B-1 shows.

Table B-1: Required Patches and Packages for Opware Agent Installation

SERVER OPERATING SYSTEM	REQUIRED PATCHES
AIX 4.3 AIX 5.1	APAR IY39444 APAR IY39429 NOTE: If AIX 4.3.3.388, 4.4.4.89, or 5.1.0.3 is installed, the Opware Agent Installer displays an error message that indicates the correct APAR to install on the server.
HP-UX (10.20, 11.00, 11.11/11i)	For HP-UX 10.20, PHCO_21018 Additionally, SW-DIST should be upgraded to the HP recommended patch level. You should continue to upgrade this package when HP recommends new versions.
Linux AS 3.0 Linux WS 3.0 Linux ES 3.0	Red Hat Enterprise Linux 3 Update 3
Solaris 10, 9, 8, 7, and 6	SUNWadmc SUNWcsl SUNWcslr (If available, depending on version) SUNWcsu SUNWesu SUNWlibms SUNlibmsr (If available, depending on version) SUNWswmt Opware strongly recommends to not remove packages from the SUNWCreq minimal required install cluster, since many packages are interdependent and operation beyond that of basic Opware functionality may be affected.
Windows 2000	Service Pack 4

Table B-1: Required Patches and Packages for Opware Agent Installation (continued)

SERVER OPERATING SYSTEM	REQUIRED PATCHES
Windows NT 4.0	Service Pack 6a

Installing an Opware Agent by using the Agent Installer CLI

The Opware Agent needs administrator-level privileges (root on Unix servers and Local System on Windows servers) to manage a server. Therefore, Opware Agent installation needs to be performed as root on Unix operating systems and as administrator on Windows operating systems.

You can install an Opware Agent on any server listed in “Supported Operating Systems for Managed Servers” in *Opware® SAS User's Guide: Server Automation*.

Perform the following steps to install an Opware Agent on a server:

- 1** Log into the server that you want to assimilate by using a remote shell.
- 2** For Unix operating systems, change the user login to root (`su - root`) and for Windows operating systems, log in as administrator.
- 3** From the Opware SAS Web Client, download the package that contains the Opware Agent Installer to a directory on the server you want to assimilate:
 1. Search for the package `opware-agent`. From the navigation panel, enter `opware-agent` in the Search box, select the Packages option, and click **Go**. The Manage Packages: Search Packages page appears.

Each operating system and operating system version has different packages for the Opware Agent Installer.

Unix:

```
opware-agent-<version>-<system_name>-<system_version>
```

Windows:

```
opware-agent-<version>-<system_name>-<system_
version>.exe
```

2. Click the package name for the Opware Agent Installer that you want to download. The Packages: Edit Properties page appears.
3. Click **Download** to save the package locally.

- 4** From the directory where the Opware Agent Installer was copied, run the Installer by entering the correct executable and options for the installation environment.

See "Example: Opware Agent Installer Command and Options" on page 532 in this appendix for more information.

Opware Agent Installer Options

When you use the Opware Agent Installer CLI, you can include the options that the following table shows to control the way that the Opware Agent is installed on a server.

Table B-2: Agent Installer Options

OPTION	DESCRIPTION
<code>--clean</code> (<code>-c</code>)	Removes any machine-specific identifying material from the server. Specifically, removes the machine ID file (MID), and all machine-specific cryptographic material. Use this option when a server is deactivated and deleted from the SAS Web Client and needs to be returned to service at a later time.
<code>-f</code>	Forces Opware Agent installation and removes the target installation directory if it exists. REQUIREMENT: When using the <code>-f</code> option, you must run the Opware Agent Installer as root on Unix operating systems and as the administrator on Windows operating systems.
<code>--logfile</code>	Specifies the path to the Opware Agent Installer log file. By default, the current directory is set as the path. By default, the log file has the following filename: <code>opware-agent-installer-<i><date></i>.log</code>
<code>--loglevel <level></code>	Sets the log level for log messages. With this option, specify one of the following levels: <code>error</code> , <code>warn</code> , <code>info</code> , <code>trace</code> , or <code>none</code> . The level <code>error</code> logs the least detail. The level <code>trace</code> logs all messages. By default, the log level is set to the log level <code>info</code> .

Table B-2: Agent Installer Options (continued)

OPTION	DESCRIPTION
-o	Logs all output to <code>stdout</code> instead of a log file. This option is invoked automatically if the default log file or the log file passed with the <code>--logfile</code> option cannot be created, for example, when running the Opware Agent Installer from non-writeable media, such as a DVD.
<code>--reconcile <type></code>	<p>Reconciles the server against any nodes assigned to the server. The <code><type></code> can be <code>full</code> or <code>addonly</code>.</p> <p><code>full</code> – All nodes in a category are selected and reconcile removes software that Opware SAS did not install.</p> <p><code>addonly</code> – Software installed outside of Opware SAS is not removed.</p> <p>WARNING: When assimilating a server that is already functioning in the operational environment, use caution when specifying the option <code>--reconcile</code>. If you specify this option, you might inadvertently uninstall software from the server.</p>
<code>--rpm bin <path></code>	<p>Specifies the path to the RPM binary to use for RPM operations. Use this option, when RPM is already installed on the server, to point the Opware Agent at the RPM binary.</p> <p>Use the <code>--withrpm</code> option to install RPM if a usable instance of RPM is <i>not</i> already installed.</p> <p>NOTE: It is unnecessary to use this option with the <code>--withrpm</code> option.</p>
-s	Starts the Opware Agent after installing it. By default, the Opware Agent Installer does not start the Opware Agent.

Table B-2: Agent Installer Options (continued)

OPTION	DESCRIPTION
<code>--template <ID></code>	<p>Assigns the nodes contained in the template to the server. <code><ID></code> can be an ID or a full name of a template.</p> <p>If this option is specified with the <code>--reconcile</code> option, Opware SAS assigns the nodes in the template to the server before reconciling the server.</p> <p>WARNING: When assimilating a server that is already functioning in the operational environment, use caution when you specify the option <code>--template</code>. If you specify this option, you might inadvertently uninstall software from the server.</p>
<code>--withmsi</code>	<p>Installs MSI 2.0 along with the Opware Agent. If MSI 2.0 is already installed, this option has no effect. Works with Windows NT 4.0 Service Pack 6a, Windows 2000, and Windows 2003.</p>
<code>--withwmi</code>	<p>Installs WMI 1.5 along with the Opware Agent. If WMI 1.5 is already installed, this option has no effect. Works with Windows NT 4.0 Service Pack 6a.</p>
<code>--withrpm</code>	<p>Installs the RPM handler with the Opware Agent. By default, an Opware Agent is not installed with this option. Opware Inc. recommends that you always include the <code>--withrpm</code> option when you install Opware Agents on Solaris servers.</p> <p>NOTE: Use the <code>--withrpm</code> option only with the Opware Agent Installers for these operating systems: Solaris 5.6, 5.7, 5.8, and 5.9, and AIX 4.3 and AIX 5.1.</p> <p>On Solaris, RPM 3.0.6 is installed in the directory <code>/opt/OPSWrpm</code> and the RPM database is installed in the directory <code>/var/opt/OPSWrpm/lib/rpm</code>.</p> <p>On AIX, RPM 3.0.5 is installed in the directory <code>/opt/freeware</code> and the RPM database is installed in the directory <code>/var/opt/freeware/lib/rpm</code>.</p>

Table B-2: Agent Installer Options (continued)

OPTION	DESCRIPTION
<code>--workdir <path></code>	Specifies the path to the Opware Agent Installer temporary working directory. Use this option if the default working directory causes problems with installation.
<code>--reboot</code>	<p>During Opware Agent Installation on a Windows server, the Agent Installer copies the <code>ogshcap.dll</code> file to the following location:</p> <pre>%SystemRoot%\system32\ogshcap.dll</pre> <p>If the file is open or is in use, the Agent Installer is unable to copy the <code>ogshcap.dll</code> file. The Agent Installer then informs the user whether to restart the machine and copies the file after restart.</p> <p>You can specify the <code>--reboot</code> Installer option in the Opware Command Line to initiate the reboot at the end of the Agent installation.</p>
<code>--resetconf(-r)</code>	Resets Opware Agent configuration file to default the settings.
<code>--no_anonymous_ssl (-A)</code>	Disables anonymous SSL. This option applies to dormant Opware Agents only. This option configures the Opware Agent so that browsers cannot connect without a valid certificate.
<code>--opsw_gw-addr-list</code>	Specifies the Opware Gateways used during Opware Agent installation.
<code>--remediate</code>	Remediates the server against any software policies attached to the server.
<code>--software_policy <id></code>	Attaches server to the software policy <ID>.
<code>--installdir <path></code>	Allows you to specify the directory where the Opware Agent will be installed. By default, the Agent is installed in <code>/opt/opware/agent</code> on UNIX, and <code>%ProgramFiles%\Opware\agent</code> on Windows.

Table B-2: Agent Installer Options (continued)

OPTION	DESCRIPTION
--no_open_fw	By default, the Opware Agent Installer will modify the Windows Firewall configuration on Windows XP and Windows 2003 (r2) servers to allow the Opware core to contact the managed server on port 1002. If you specify this option, the firewall configuration will not be modified. The server may not be manageable by Opware in this case.
--settime (-t)	<p>Synchronizes the time on the server on which the Opware Agent is installed with that of the Opware core.</p> <p>NOTE:</p> <p>If the server on which the Opware Agent is being installed is significantly ahead of the clock on the Opware core, then the clock on the managed server is set back in time. Since this can cause problems, do not use the --settime option unless you are sure that this scenario is not a problem in your environment.</p> <p>If a managed server's clock is significantly behind of the clock on the Opware core, the Opware Agent installation might fail. To install an Opware Agent successfully, use the --settime option or manually set the time and date on the managed server before retrying the Opware Agent installation.</p>

Example: Opware Agent Installer Command and Options

Enter the following command and options to install the Opware Agent for Solaris 5.7 in the default directories and log the results of the installation in the log file:

```
% opsware-agent-14.2.12.5-solaris-5.7 --logfile opsware-agent-
installer.log --loglevel info
```

Enter the following command and options to install the Opware Agent for Windows NT 4.0 in the default directories and log the results of the installation in the log file:

```
% opsware-agent-14.2.12.5-win32-4.0.exe --logfile opsware-
agent-installer.log --loglevel info
```

Starting an Opsware Agent on a Server

If you do *not* include the `-s` option on the command line when you install an Opsware Agent, you have to start the Opsware Agent on the server manually.

Enter the following command, which varies with the operating system:

Solaris:

```
/etc/init.d/cogbot start
```

Linux:

```
/etc/rc.d/init.d/cogbot start
```

AIX:

```
/etc/rc.d/init.d/cogbot start
```

HP-UX:

```
/sbin/init.d/cogbot start
```

Windows:

```
net start shadowbot
```

Verifying Opsware Agent Functionality

Perform the following steps to verify Opsware Agent functionality:

- 1** From the navigation panel in the SAS Web Client, click Servers ► Manage Servers. The Manage Servers page appears. Browse the list to find the server whose Opsware Agent installation you want to verify. If necessary, select the correct customer and facility for the server and click **Update**.

Or

Search for the server whose Opsware Agent installation you want to verify.

Or

- 2** Verify that the server appears in the Manage Servers list and has the correct properties.

See “Using the Search Feature” and “Server Searching by IP Address” in *Opsware® SAS User’s Guide: Server Automation* for more information.

- 3** If you want to discover reasons why a server is unreachable, you can run a Communication Test. See “Agent Reachability Communication Tests” on page 125 in Chapter 4 for more information.

Augmenting the Information for a Managed Server



Use caution when you augment the discovery process for an Opware-managed server that is functioning in the operational environment. You might inadvertently install or uninstall software from the server. During the test remediate, verify what software will be uninstalled from the server before you perform the actual remediate operation.

Perform the following steps to augment the information for an Opware-managed server:

- 1** Model the OS and other applications running on the server in Opware SAS by defining the OS with the Prepare Operating System Wizard and by creating nodes and templates for applications running on the assimilated server.

See the *Opware® SAS Policy Setter's Guide* for more information about Operating System Definitions.
- 2** Move the server to the appropriate nodes for the OS and installed applications.

The server is tracked in the SAS Web Client; however, the server operating system *cannot* be managed while the server is assigned to the generic operating system node. You must reassign the server to the operating system that was defined with the OS Provisioning feature.
- 3** Remediate the server.
- 4** If an IP range group was set up, servers are automatically associated with customers when users install an Opware Agent on the servers. Otherwise, the servers are associated with the Not Assigned customer. To change the customer associated with a server, See “Editing the Properties of a Server” on page 320 in Chapter 8 for more information.
- 5** To specify the server's use, stage, and state, edit the server's properties. See “Editing the Properties of a Server” on page 320 in Chapter 8 for more information.

Discovery is complete. Opware SAS assumes that the server should always be running the specific OS build it has been associated with. Any changes to the OS outside of Opware SAS are not captured in the model.

Users can deploy and manage new applications on the server, just as if Opware SAS initially provisioned the server. Users can also deploy OS level patches on the server, or rebuild the OS by using the OS build with which the server was associated.

Uninstalling an Opsware Agent on Unix and Windows



To uninstall Opsware Agents on Windows NT, Windows Scripting Host 5.1 or Internet Explorer 5.5 must be installed on Windows NT.

Perform the following steps to uninstall an Opsware Agent on Unix or Windows:

- 1** Log into Unix as root user. Log into Windows as Administrator.
- 2** Change directories to any directory other than the Opsware Agent's installation directory.

- 3** On Unix, enter the following command:

```
<installation_directory>/bin/agent_uninstall.sh
```

By default, for Solaris and AIX, the Opsware Agent Uninstaller will not remove the Opsware RPM package. For command line options for the agent uninstaller, including how to activate removal of the Opsware RPM package, See “Opsware Agent Uninstaller Options” on page 535 in this appendix for more information.

- 4** On Windows, enter the following command:

```
msiexec /x <installation_directory>\bin\agent_uninstall.msi
```

- 5** As the uninstall proceeds, the Unix platform `stdout` shows the uninstallation progress. The Windows uninstall does not show uninstallation progress.

Opsware Agent Uninstaller Options

When you use the Opsware Agent Uninstaller, you can include the options that Table B-3 and Table B-4 show.

Table B-3: Opsware Agent Uninstallation Unix Options

OPTION	DESCRIPTION
<code>--uninstallerVersion</code>	Show the uninstaller version.
<code>--help</code>	Show this help.
<code>--no_deactivate</code>	Do not deactivate the server; by default, the server is deactivated.

Table B-3: Opware Agent Uninstallation Unix Options (continued)

OPTION	DESCRIPTION
<code>--force</code>	Do not prompt for confirmation before deactivating the server.
<code>--delete_opsw_rpm</code>	Remove the OPSW RPM package (AIX, Solaris only). Use the following commands to remove the RPM package: Solaris: <code>pkgrm -n OPSWRpm</code> AIX: <code>installp -u rpm.rte</code>

Table B-4: Opware Agent Uninstallation Windows Options

OPTION	DESCRIPTION
<code>NO_DEACTIVATE="1"</code>	Do not deactivate the server; by default the server is deactivated.
<code>FORCE="1"</code>	Do not prompt for confirmation before deactivating the server.

During Opware Agent Uninstallation on a Windows server, the Agent Installer removes the `ogshcap.dll` file from the following location:

```
%SystemRoot%\system32\ogshcap.dll
```

If the file is open or is in use, the Agent Installer is unable to remove the `ogshcap.dll` file. The Agent Installer then prompts the user to restart the machine and removes the file after restart.

Uninstalling Earlier Versions of Opware Agents on Unix

Perform the following steps to uninstall Opware Agents versions 5.1 and earlier:

- 1 Stop the Opware Agent on the server by running the following command as root:

Linux:

```
/etc/rc.d/init.d/cogbot stop
```

Solaris:

```
/etc/init.d/cogbot stop
```

HP-UX:


```
/sbin/init.d/cogbot stop
```

AIX:

```
/etc/rc.d/init.d/cogbot stop
```

2 Deactivate or delete the server by using the **SAS Web Client Server** menu.

3 For Linux servers only, run `chkconfig` to de-register the Opware Agent initialization script:

```
% /sbin/chkconfig -del cogbot
```

4 As root, delete the following files and directories to remove the Opware Agent files from the server:

Linux:

```
/etc/rc.d/init.d/cogbot
```

Solaris:

```
/etc/init.d/cogbot
```

```
/etc/rc2.d/S79cogbot
```

```
/etc/rc0.d/K44cogbot
```

HP-UX:

```
/sbin/init.d/cogbot
```

```
/sbin/rc2.d/cogbot
```

AIX:

```
/etc/rc2.d/init.d/cogbot
```

```
/etc/rc.d/S79cogbot
```

All Unix:

```
/opt/OPSW
```

```
/var/lc
```

Uninstalling Earlier Versions of Opware Agents on Windows

Perform the following steps to uninstall earlier versions of Opware Agents on Windows:

1 Stop the Opware Agent by running the following command as administrator:

```
C:\> net stop shadowbot
```

2 Deactivate or delete the server by using the **SAS Web Client Server** menu.

3 Deregister the Opware Agent service by running the following command as administrator:

```
C:\> "%SystemDrive%\Program  
Files\Loudcloud\blackshadow\watchdog\watchdog.exe" -x
```

4 As administrator, delete the following directories to remove the Opware Agent:

```
"%SystemDrive%\Program Files\Loudcloud"  
"%SystemDrive%\Program Files\Common Files\Loudcloud"
```

Opware Agent Upgrade Tool

This section contains the following topics:

- Ways to Upgrade Opware Agents
- Prerequisites for Using the Opware Agent Upgrade Tool
- Upgrading the Opware Agent on Managed Servers
- Commands for the Opware Agent Upgrade Tool
- Options for the Opware Agent Upgrade Tool
- Example: Options for the Opware Agent Upgrade Tool
- Example: Commands and Output for Agent Upgrade Tool

Ways to Upgrade Opware Agents

After you upgrade Opware SAS running in a facility, you should upgrade the Opware Agents on every managed server to the new version, so that you can utilize the new features in the newly-upgraded core.

Opware SAS features continue to work on a managed server even when it is running an older Opware Agent. However, new features in the new versions might not be available for that server.

Refer to the Release Notes for the new version for information about the compatibility of new features with older agents.

You can upgrade the Opware Agents on managed servers in the following ways:

- Use the Opsware Agent Installer (a command line interface) to install a new Opsware Agent on one server at a time.

See “Agent Installation Using the CLI” on page 521 in this appendix for information about how to use the Opsware Agent Installer.

- Use the Opsware Agent Upgrade Tool to upgrade Opsware Agents on groups of servers. Running the tool upgrades deployed Opsware Agents on managed servers. You can run the script simultaneously on many servers to upgrade large groups of Opsware Agents.

The Opsware Agent Upgrade Tool has the following characteristics:

- It is a command line interface that provides a flexible mechanism for selecting servers to upgrade, and for monitoring and reviewing upgrade operations.
- You can use it to upgrade many Opsware Agents on managed servers simultaneously.
- It runs within your preferred Unix shell, allowing it to leverage the power of standard Unix shells and text processing tools.
- You can use it to upgrade a server in any facility running Opsware SAS. You can run it from an Opsware shell attached to any Opsware SAS in any facility.

The Opsware shell is a program that authenticates users in Opsware SAS, starts the user’s normal Unix shell (as specified in the standard password database). Using the Opsware shell allows the user to run the Opsware Agent Upgrade Tool in this facility.

Prerequisites for Using the Opsware Agent Upgrade Tool

- On a core server of the facility being upgraded, install the Opsware Shell RPM by downloading the `opsh` package from the SAS Web Client. See the *Opsware® SAS Content Migration Guide* for instructions on downloading a package.

Installing the `opsh` RPM places the Opsware shell and the Opsware Agent Upgrade Tool in the directory `/opt/OPSWopsh/bin`.

- You need the correct permissions to upgrade Opsware Agents. Run the Opsware shell by specifying the Opsware `admin` user and password to ensure that you have the appropriate permissions. (Contact your Opsware administrator to obtain the password.)

When you start an Opsware shell to run the Opsware Agent Upgrade Tool, the user name and password are authenticated by Opsware SAS.

- The server where you install the `opsh` RPM must be able to resolve the name `way.<facility-domain>` to the host running the Command Engine in the facility’s

core. For example, if the Command Engine runs on a host in the `prod.opware.com` domain, the servers must resolve the name `way.prod.opware.com`. You specified the `facility-domain` when you installed the core.

Upgrading the Opware Agent on Managed Servers

To upgrade the Opware Agent, perform the following steps:

- 1** After you install the `opsh` RPM on a core server, enter the following command as root to start the Opware shell:

```
opsh [username@] facility-domain
```

For example:

```
opsh admin@prod.opware.com
```

See the preceding section for the name resolution requirement for `facility-domain`. See “Commands for the Opware Agent Upgrade Tool” on page 541 for more information on `opsh`.

- 2** (Optional) To obtain information about the current Opware Agents running on the managed servers before you upgrade them, enter any of the following commands and options:

```
opsh_agent query server-options
```

(Enter this command if you want to view a report of the Opware Agent versions running on the servers before you upgrade them.)

```
opsh_agent verify server-options schedule-options \  
agent-version
```

(Enter this command if you want to verify the versions of the Opware Agents running on the managed servers before you upgrade them.)

- 3** To upgrade Agents on specified servers, enter the following Opware Agent Upgrade Tool commands and options:

```
opsh_agent stage server-options schedule-options \  
[--always] agent-version
```

(Enter this command if you want to download the package for the Opware Agent to the managed server before you run the upgrade.)

```
opsh_agent upgrade server-options schedule-options \  
agent-version
```

```
[--always] agent-version
```

- 4** (Optional) To review the status of the Opware Agent upgrade, enter the following command and option:

```
opsh_agent review session-id
```

Commands for the Opware Agent Upgrade Tool

- `opsh [username@] facility-domain`

This command starts an Opware shell and authenticates the user name against the Opware facility running at the specified domain.

If you do not specify a user name, the currently logged in user name is used. The Opware shell prompts for a password.

A new Unix shell (which is attached to the specified Opware core-domain) is started. (The password database for the user specifies which Unix shell to use.)

- `opsh_agent query server-options`

This command must be run from an Opware shell started with the `opsh` command.

This command queries the reported version of Opware Agents and any staging status for the specified servers by examining data in the Model Repository.

One line is printed to stdout for each server that shows device ID, IP address, current Opware Agent version, and any staging status.

You can specify the servers by using the `--device`, `--customer`, `--facility`, and `--os` options.

- `opsh_agent stage server-options schedule-options \`
`[--always] agent-version`

You must run this command from an Opware shell started with the `opsh` command.

This command contacts the Opware Agent on each specified server and instructs it to download the package for the specified version of the Opware Agent from the Software Repository.

If the download is successful, the staging status is written to the Model Repository for the server.

To download the package to the server even when this command was entered previously (recorded in the Model Repository), specify the `--always` option.

One line is printed to stdout for each server that shows the device ID, IP address, and a success or failure indicator.

You can specify the servers by using the `--server`, `--customer`, `--facility` and `--os` options.

A session is started and the session ID displays for later review. After the session ID displays, you can type CTRL-C and review the session later using the `opsh_agent review` command.

- `opsh_agent upgrade server-options schedule-options \`
 `[--always] agent-version`

You must run this command from an Opware shell started with the `opsh` command.

This command contacts the Opware Agent on each specified server and instructs it to upgrade to the specified version. If the necessary package has not been downloaded on the server already (the `opsh_agent stage` command was entered), the package is downloaded from the Software Repository.

If the upgrade is successful, the package is removed from the server and the staging status is deleted from the Model Repository.

To upgrade the Opware Agent even when the specified version of the Opware Agent was already installed on the managed servers, enter the `--always` option. (The Model Repository records when Opware Agents are upgraded on servers.)

One line is printed to stdout for each server that shows the device ID, IP address, and a success or failure indicator.

You can specify the servers by using the `--server`, `--customer`, `--facility`, and `--os` options.

A session is started and the session ID displays for later review. After the session ID displays, you can type CTRL-C and review the session later by using the `opsh_agent review` command.

- `opsh_agent verify server-options schedule-options \`
 `agent-version`

You must run this command from an Opware shell started with the `opsh` command.

This command contacts the Opware Agent on each specified server to verify that it is running the specified version.

One line is printed to stdout for each server that shows the device ID, IP address, the word OLD, NEW, or CURRENT and the actual Opsware Agent version running on the server.

You can specify the servers by using the `--server`, `--customer`, `--facility`, and `--os` options.

A session is started and the session ID displays for later review. After the session ID displays, you can enter CTRL-C and review the session later by using the `opsh_agent review` command.

- `opsh_agent review session-id`

You must run this command from an Opsware shell started with the `opsh` command; although, not necessarily the same Opsware shell from which the original command was started.

This command attaches to a running `opsh_agent stage`, `opsh_agent upgrade` or `opsh_agent verify` session running on the Command Engine. It prints the same output to stdout that the original command would have printed if the user had not typed CTRL-C and terminated the command. If the session is complete, it shows the same results that were shown when the session completed.

Options for the Opsware Agent Upgrade Tool

Server-options: `--server|-S <svr-spec> --customer|-C <cust-spec> --facility|-F <fac-spec> --os|-O <os-spec>`

If more than one of the `--customer`, `--facility`, or `--os` options is specified, only servers that match all options are selected. Any servers specified by using the `--server` option are added to (or subtracted from) the list specified by combining the `--customer`, `--facility`, and `--os` options.

Table B-5: Options for the Opsware Agent Upgrade Tool

LONG OPTION	SHORT OPTION	VALUE	MEANING
<code>--server</code>	<code>-S</code>	<code><svr-spec></code>	Server by device ID, IP address, or system name
<code>--customer</code>	<code>-C</code>	<code><cust-spec></code>	All servers associated with the customer specified by the customer ID or name

Table B-5: Options for the Opware Agent Upgrade Tool (continued)

LONG OPTION	SHORT OPTION	VALUE	MEANING
--facility	-F	<fac-spec>	All servers in the facility specified by the facility ID or name
--os	-O	<os-spec>	All servers running the operating system specified by the OS name

Schedule-options: --when|-W when-time --until|-U until-time

Table B-6: Schedule Options

LONG OPTION	SHORT OPTION	VALUE	MEANING
--when	-W	<when-time>	<p>Start time for a stage, upgrade, verify, or test operation in the format:</p> <p>MM/DD/YYYY-HH:MM</p> <p>If the --when option is used, the operation starts at the specified time, but the command displays a session ID and returns immediately.</p> <p>When you schedule an operation, you use the <code>review</code> command to review the results after the operation has run.</p> <p>If the --when option is not specified, the operation starts immediately and the command displays the output of the command.</p>
--until	-U	<until-time>	<p>End time for a stage, upgrade, verify or test operation in the format:</p> <p>MM/DD/YYYY-HH:MM</p> <p>If the --until option is specified, the operation stops processing servers at the specified time. Any servers that are not complete are left in a consistent state; this might require that the session run past the specified time.</p>

Miscellaneous options:

```
--ip|-I --always|-A --parallel|-P --theword|-T
```

Table B-7: Miscellaneous Options

LONG OPTION	SHORT OPTION	VALUE	MEANING
--ip	-I	(N/A)	Display IP addresses instead of host names.
--always	-A	(N/A)	Always stage or upgrade servers even if the current version is staged or upgraded.
--parallel	-P	<Concurrency>	The maximum of concurrent commands. (Recommended default = 10)
--theword	-T	<hostname>	The host name or IP address to use when contacting the Software Repository from a server.

Example: Options for the Opsware Agent Upgrade Tool

The following table provides examples for running the Opsware Agent Upgrade Tool.

Table B-8: Examples of Options for the Opsware Agent Upgrade Option

EXAMPLE	DESCRIPTION
--server 1,2	Selects servers 1 and 2.
--facility Y,Z	Selects all servers (for all customers) in facilities Y and Z.
--customer -A,-B --facility Z	Selects all servers in facility Z except those owned by customers A and B.
--server 1,2,-3,-4 --customer A,B --facility Y,Z	Select servers 1 and 2 as well as all servers owned by customers A or B which are in facilities Y or Z except servers 3 and 4.
--server 1,-2 --customer A,B --facility -Y,-Z --os SunOS 5.8	Select server 1 and all servers owned by customers A or B, except those in facilities Y or Z and which are Solaris 5.8 machines excluding server 2.

Example: Commands and Output for Agent Upgrade Tool

```
# cd /opt/OPSWopsh/bin
# ./opsh admin@prod.opsware.com
admin@prod.opsware.com's password:
#
# ./opsh_agent verify --os "SunOS*" 14a.2.12.18
Session 37802500101L
Device ID Name/IP address Version Result Status Reason
410101L core2-1.prod.opsware.com 14a.2.12.18 CURRENT SUCCESS
^C
Interrupted review of running session 37802500101L
Use review 37802500101L command anytime to review session status
#
# ./opsh_agent review 37802500101L
Session 37802500101L
Device ID Name/IP address Version Result Status Reason
410101L d033.prod.opsware.com 14a.2.12.18 CURRENT SUCCESS
670101L dhcp-174.prod.opsware.com 14a.2.12.16 OLDER SUCCESS
1460100L emb218-37.manu.opsware.com 14a.2.12.18 CURRENT SUCCESS
20100L f001.manu.opsware.com 14a.2.12.18 CURRENT SUCCESS
10100L f002.manu.opsware.com 14a.2.12.21 NEWER SUCCESS
210100L m022.manu.opsware.com 14a.2.12.18 CURRENT SUCCESS
Session 37802500101L completed.
```

Opware Agent Upgrade Custom Extension

Opware SAS includes a custom extension ("AgentUpgrade") that you can use to upgrade Opware Agents from the previous three versions.

The Custom Extension feature is accessed through the Run Custom Extension Wizard. This Wizard allows a user to choose a custom extension to run, specify necessary input data for the extension, validate the data required to run the extension, run the extension, and view or download the results from the job. When a user runs a custom extension, the job shows up in My Jobs.

To access the Run Custom Extension Wizard, users must be assigned to a user group that has the permission Wizard: Opware Extension. When users have this permission, they can run any custom extensions on the servers they have access to in the SAS Web Client.

See Chapter 11, "Opware SAS Custom Extensions" on page 428 of this guide for more information.

Any user who has the ability to run custom extensions can run the Agent Upgrade Custom Extension.

The Agent Upgrade custom extension only upgrades agents that are not up-to-date. Therefore, rerunning the custom extension on a group of servers will not affect servers that are already running the most recent version of the Opware Agent.

Upgrading Agents with the Agent Upgrade Custom Extension

To run the Agent Upgrade custom extension, perform the following steps:

- 1** From the SAS Web Client home page, click the Run Custom Extensions link in the Tasks panel.

Or

From the navigation panel, click Servers ► Manage Servers. The Manage Servers list appears. Select the servers on which you want to run a custom extension and choose **Run Extension** from the **Tasks** menu.

The Run Custom Extension Wizard appears.

- 2** Select the "AgentUpgrade" custom extension and click **Next**.

If you have not already selected servers from the Manage Servers list, the Select Servers page appears.

- 3** If prompted, select the servers or groups on which you want to run the custom extension and click **Next**. You can find the servers that you want to run a custom extension on by browsing the list or by searching.

The Agent Upgrade Settings page appears as shown in Figure B-12:

Figure B-12: Specify Settings Page for the Agent Upgrade Custom Extension

Specify Settings

Enter values for each field (**bold items are required**) to run this extension. Mouse over the note icon (📄) for directions on setting the values correctly.

AgentUpgrade

Operation Mode: Stage Package (dropdown) 📄

Agent Version: 32a.0.1.78 (dropdown) 📄

Flags to pass to the agent installer: (text input) 📄

Perform stage/upgrade even if not needed: Yes No 📄

- 4 Specify the settings for the custom extension and click **Next**.
 - Select the Agent Upgrade action you want to perform:
 - **Stage Package**: Downloads the Opware Agent Installer package (the binaries) but does not upgrade the Opware Agent.
 - **Perform Upgrade**: Upgrades the servers to the specified Opware Agent version by downloading the Agent Installer package (binaries) if not previously staged. If the Agent Installer package was already staged, upgrades the Opware Agent version by using the staged version of package on the server.
 - **Verify Upgrade**: Check whether all the servers are running the selected Opware Agent version.
 - Select the Opware Agent version to upgrade to. All agent versions available in the Software Repository are displayed in the list. By default, the latest version available in the Software Repository is selected.
 - Enter additional parameters to pass to the Opware Agent Installer. The Agent Upgrade custom extension does not validate the parameters you enter. See “Opware Agent Installer Options” on page 528 in this chapter for information about the parameters you can enter in this field.

- Specify whether the custom extension should upgrade Opsware Agents even if the version of the currently running agent is equal to or greater than the version being upgraded to.

The Confirm Settings Screen appears and displays the selected options.

- 5 Review the values that you entered and the servers that you selected on which to run the Agent Upgrade custom extension. (You can remove servers from the list by deselecting their check boxes. Click the “Show remaining servers” link to display the complete list of selected servers.)

- 6 Click **Next**.

- 7 On the Schedule and Notify page, you have the following options:

- **Notify:** Choose the Condition option and set the parameters to send an email when the operation is completed. You can choose to have an email sent on any result, if the operation fails, or if the operation is successful. To add another email recipient, click the plus (+) button next to the Recipients field.
- **Schedule:** Choose either **Run Now** to execute the operation immediately, or choose **Specify Time** to schedule the operation for a later time.

When you schedule a job for a server group, you can specify how the members of the group are determined. The membership of a dynamic server group changes based on the changes in your operational environment. If you have “Allow Run Refresh Jobs” permissions, you will see additional options. Select either of the following options:

- **Option 1:** Membership is determined based on the “Time of Confirm Selection.” Select this option to run the job on the servers that were in the group when you scheduled the job. Changes to the group membership do not affect the list of the servers that the job will run on.
- **Option 2:** Membership is updated when the job runs. Select this option to recalculate the group membership prior to running the job. Changes to group membership are reflected in the list of servers that the job will run on.



The time used for the scheduled job is specified in your preferred time zone which can be modified in My Profile. If you do not have the preferred time zone set, the time zone is derived from the Opsware SAS core server (usually UTC).

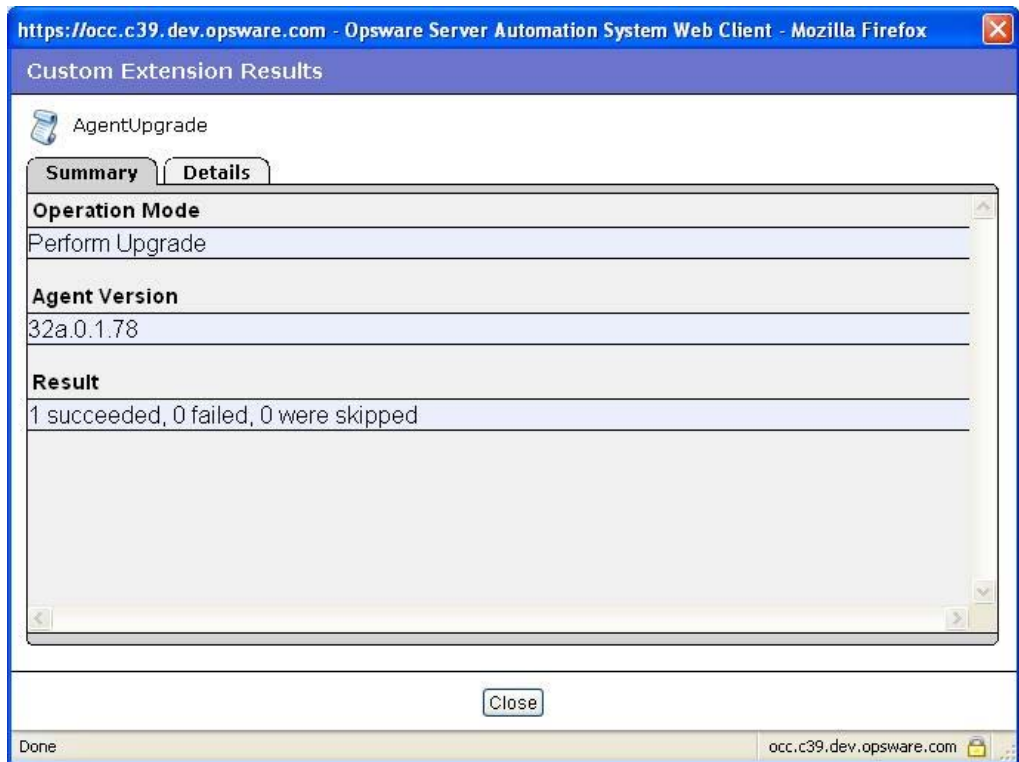
- 8 Click **Run** to start the Custom Extension Wizard.

If you selected to run the job at that time, a progress bar appears for the servers on which the extension is running that shows the progress of the job.

- 9 When the custom extension finishes running, you can click **View Details** to see the results. The Custom Extension Results window appears. The results window contains a tab for the operation summary and a tab for the operation details.

By default, the Summary tab is displayed.

Figure B-13: Summary Tab in the Details Window of the Agent Upgrade Custom Extension

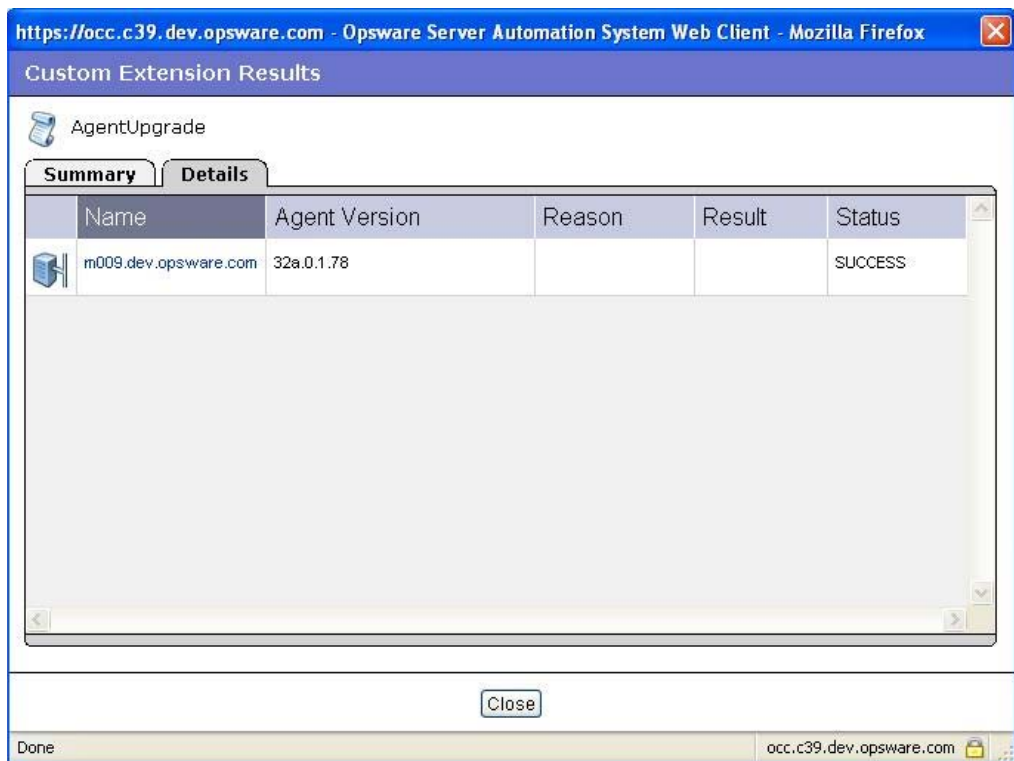


The Details tab contains a table with one row for each server selected. The table in each tab includes the following columns:

- **Name:** The name of the server
- **Agent Version:** The agent version running on the server after the custom extension completes
- **Reason:** If an operation failed, a text description of the reason the operation failed

- **Result:** (Only shown for Verify operations) Shows the result of the verification:
 - **OLDER:** The agent on the server is older than the selected version
 - **UP TO DATE:** The agent on the server is up to date
- **Status:** The exit status of the command SUCCESS or FAILURE

Figure B-14: Details tab in Results Window for the Agent Upgrade Custom Extension



- 10** When you are done viewing the results, click **Close** to close the window.

After you close the wizard, you can view the progress of the custom extension by viewing My Jobs (accessible from the Home page or the navigation panel). Each custom extension job is identified with the name Run Custom Extension. Click the name link to identify which extension was run.

See “Server Management Scheduling and Notification” on page 330 in Chapter 8 for information about the My Jobs feature.

Appendix C: Global Shell Utilities Syntax

IN THIS APPENDIX

This section discusses the following topics:

- aaa Utility
- rosh Utility
- swenc Utility

aaa Utility

The `aaa` utility grants and revokes permissions for operations that use the OGFS. For example, the `aaa` utility grants permission for the `readServerFilesystem` operation, allowing you to browse a server's file system in the SAS Client. To run the `aaa` utility, you must belong to the Administrators user group.

The permissions granted and revoked by the `aaa` utility are stored in the `/opsw/Permissions` directory of the OGFS. For details on the contents of the directory, see “`/opsw/Permissions Directory`” on page 575.

aaa Syntax

The `aaa` utility has the following syntax:

```
aaa shell-perm (grant | revoke) -o operation [-u user-group]
[-f facility | -c customer | -g device-group [-s | -l login]]
```

Table C-1 describes the command options and Table C-2 lists the operations that can be granted or revoked the `aaa` utility.

Table C-1: `aaa` Options

OPTION	DESCRIPTION
<code>-o operation</code>	The operation on which to grant or revoke the permission. For a list of allowed values, see the Operation column in Table C-2.

Table C-1: *aaa* Options

OPTION	DESCRIPTION
<code>-u <i>user-group</i></code>	The Opsware user group that is assigned the permission. This value is inferred from the current working directory if it corresponds to a user group. If it cannot be inferred, specify a user group.
<code>-f <i>facility</i></code>	The name, ID, or path to a facility, such as: <code>/opsw/Facility/Chicago</code> Permission will be granted to all servers in this facility.
<code>-c <i>customer</i></code>	The name, ID, or path to a customer, such as: <code>/opsw/Customer/Alpha</code> Permission will be granted to all servers that belong to this customer.
<code>-g <i>device-group</i></code>	The name, ID, or path to a public device group, such as: <code>/opsw/Group/Public/Unix Servers</code> Permission will be granted to all servers that belong to this group. To specify the device group by name, omit the following: <code>/opsw/Group/</code>
<code>-l <i>login</i></code>	A login account on the servers that are specified by the <code>-f</code> , <code>-c</code> , or <code>-g</code> option. On a Unix server, for example, the <i>login</i> is the Unix user name. Login accounts with multi-byte characters are not supported.
<code>-s</code>	The login account on the servers (specified by <code>-f</code> , <code>-c</code> , or <code>-g</code>) is the same as the Opsware user name.

aaa Usage Rules

The following usage rules and recommendations apply to the *aaa* utility:

- For operations that are performed on a server, one of the `-f`, `-c`, or `-g` options is required.
- As a best practice, when you are granting permissions, use care when you select servers so that you do not capture more servers than you intend. This is particularly important when using the `-c` or `-f` option. For example, if you want to grant permission to the `loginToServer` operation for all servers in the `Chicago` facility as `root`, you could use the `-f` option to select all servers in a particular facility. However, this may also select Windows servers, which is probably not desired since the `root` user does not typically exist on Windows servers. In this case, you should define a public device group that only includes servers in the `Chicago` facility which are running a Unix operating system.
- If you specify the `-f`, `-c`, or `-g` option, you must also specify either the `-s` or `-l` option. The choice of the `-s` or `-l` option depends on the policies of your organization. If users log into managed servers with generic user names (such as `root`), then you should specify the `-l` option. If users log into managed servers with individual user names, which are the same as their Opsware user names, they should specify the `-s` option.
- The `-f` and `-c` options are provided as a convenience; however, in general, it is recommended that you define permissions based on device groups instead.
- The `revoke` command can only remove a permission that was previously granted. If the permission was not previously granted, the `revoke` command has no effect.
- The `revoke` command only removes a permission for a specific user group. If a user has overlapping permissions, revoking permissions from a single user group will not prevent the user from performing that operation. For example, suppose a user belongs to two user groups that both have the `launchGlobalShell` permission. If this permission is revoked from only one of those user groups, the user still has the `launchGlobalShell` permission.

aaa Examples

The following example gives all members of the `Advanced Users` group permission to open a Global Shell session:

```
aaa shell-perm grant -o launchGlobalShell \  
-u 'Advanced Users'
```

The following command allows members of the `Advanced Users` group to view the file systems as `root` of all Unix servers:

```
aaa shell-perm grant -o readServerFilesystem \  

```

```
-u 'Advanced Users' -g 'Public/All Unix Servers' -l root
```

The next example gives all members of the `Unix Admin` user group permission to log in as `root` to all servers in the `Public/Trading Servers` device group:

```
aaa shell-perm grant -o loginToServer -u 'Unix Admin' \  
-g 'Public/Trading Servers' -l root
```

The following example allows the `Advanced Users` group to run commands as `root` on servers associated with the `Acme Inc` customer.

```
aaa shell-perm grant -o runCommandOnServer \  
-u 'Advanced Users' -c 'Acme Inc' -l root
```

The next example removes the permission for the `Unix Admin` user group to log into servers that belong to the device group named `Public/Unix Servers`. The command applies to any login, because the `-l` option is not specified.

```
aaa shell-perm revoke -o loginToServer -u 'Unix Admin' \  
-g 'Public/Unix Servers'
```

Global Shell Operations (Permissions)

The actions that an Opware user can perform within the Global Shell are determined by the operations specified by the `aaa` utility. Most of these operations, such as `readServerFilesystem`, can be granted on both managed servers and on a login basis. The login is the user name on the managed server, such as the `Administrator` user on Windows or `root` on Unix.

A login is not specific to a particular platform (operating system). For example, if the permissions specify that a user can read the file system as `root`, then `root` will appear under the `files` subdirectory, regardless of the platform. The Server Explorer of the SAS Client displays the login names that you have been authorized to access that server's file system.

The operations are listed in the `/opsw/Permissions` directory of the OGFS.

Table C-2 identifies and describes the server operations in Global Shell. In the table, the On Server column identifies which operations can be granted for a set of managed servers, and the On Login column identifies the operations that can be granted for specific logins (users).

Table C-2: Global Shell Operations

OPERATION (PERMISSION)	DESCRIPTION	ON SERVER	ON LOGIN
launchGlobalShell	Launches the Global Shell.	No	No
loginToServer	Opens a shell session on a Unix server. In the SAS Client, this is the Remote Terminal feature that opens a terminal window for a Unix server.	No	No
readServerComplus	Reads COM Plus objects as a specific login. In the SAS Client, use the Server Explorer to browse these objects on a Windows server.	Yes	Yes
readServerFilesystem	Reads a managed server as a specific login. In the SAS Client, use the Server Explorer to browse the file system of a managed server.	Yes	Yes
readServerMetabase	Reads IIS Metabase objects as a specific login. In the SAS Client, use the Server Explorer to browse these objects on a Windows server.	Yes	Yes
readServerRegistry	Reads registry files as a specific login. In the SAS Client, use the Server Explorer to view the Windows Registry.	Yes	Yes
relayRdpToServer	Opens an RDP session on a Windows server. In the SAS Client, this is the Remote Terminal feature that opens an RDP client window for a Windows server.	No	No

Table C-2: Global Shell Operations (continued)

OPERATION (PERMISSION)	DESCRIPTION	ON SERVER	ON LOGIN
runCommandOnServer	Runs a command or script on a managed server using a <code>rosh</code> operation, where that command or script already exist. In the SAS Client, this is used for Windows Services when you use the Server Explorer.	Yes	Yes
runTrustedOnServer	Only for internal use by Opware SAS. Do not use this operation. Opware SAS uses this operation for scripts in <code>/opsw/Script/Shared</code> , which implement certain Opware SAS features. These scripts are provided with Opware SAS and cannot be created or modified by users.	Yes	Yes
writeServerFilesystem	Modifies files on a managed server as a specific login. In the SAS Client, use the Server Explorer to modify the file system of a managed server.	Yes	Yes

rosh Utility

The Remote Opware Shell (`rosh`) command makes a client connection that enables you to remotely run programs on managed servers. You invoke the `rosh` command from within a Global Shell session.

rosh Syntax

For servers, the `rosh` command has the following syntax:

```
rosh (-n server-name | -i server-id) [-d dir] [-l login-name]
[-s] [-t | -T] [command [arg ...]]
```

For network devices, the `rosh` command has the following syntax:

```
rosh (-n device-name | -i device-id) [-N] [-C comment]
[-L] [-P parameters] [-s] [-V variables] [command [arg ...]]
```

Table C-3 describes the `rosh` options of the preceding syntax statements.

Table C-3: *rosh* Options and Commands

OPTION	DESCRIPTION
<code>-C comment</code>	A comment for the log of a network script invocation.
<code>-d dir</code>	Sets the working directory (path) on the remote server. The default is the remote user's home directory.
<code>-i server-id</code>	Specifies the server by its ID, which must already exist in the <code>/opsw/.Server.ID</code> directory.
<code>-l login-name</code>	Specifies the login name of the remote user who performs operations on a remote server, which must already exist in the <code>/opsw/Server</code> directory.
<code>-L</code>	The network script should be run line-by-line.
<code>-m</code>	Network device mode.
<code>-n server-name</code>	Specifies the server by its name, which must already exist in the <code>/opsw/Server</code> directory.
<code>-N</code>	The <code>-i</code> or <code>-n</code> option refers to a network device instead of a server.
<code>-P parameters</code>	Parameters for a network advanced script.
<code>-r</code>	Relays RDP data to a managed server (on Windows).
<code>-s script-name</code>	Treats a command as the name of a saved script that will be sent to and run on the remote server.
<code>-t</code>	Forces the remote session to run in a pseudo terminal (for Unix servers only).
<code>-T</code>	Forces the remote session to run without a pseudo terminal (for Unix servers only).
<code>-V variables</code>	Variables for a network command or advanced script.
<code>-w seconds</code>	Inactivity timeout.
<code>-W seconds</code>	Overall timeout.
<code>command</code> <code>[args . . .]</code>	Runs a program or saved script.

rosh Usage Rules

The following usage rules apply to the `rosh` program:

- Specify either the `-n` or `-i` option to log into or run programs on a managed server. These options are mutually exclusive, but if both are specified the `-i` option has precedence.
- If neither the `-n`, `-i`, and `id` options are specified, the managed server can be inferred if your working directory is at or below:

```
/opsw/Server/.../server-name/
```

Or

```
/opsw/.Server.ID/server-id/
```

- If `-r` is specified, no other option (excluding `-n` or `-i`) can be specified.
- If `-l` is not specified, the login-name can be inferred if your working directory is at or below:

```
/opsw/Server/.../server-name/files/login-name/
```

Or

```
/opsw/.Server.ID/server-id/files/login-name/
```

- If `-s` is specified and `command` is a saved shared script with a `setuid` policy, the login-name specified by the `-l` option will be overridden. In this case, the `-l` option may be omitted. These scripts are stored in `/opsw/Script/Shared`.
- If your working directory is not below `server/files/login-name` and `-d` is not specified, the `cwdpath` defaults to the home directory for `login-name`. To default to the home directory, you must specify `-l`.
- For network scripts, if your current working directory is below a network device directory in the OFGS, you do not need to specify the device with `-N`, `-n` or `-i`. The network device is implied by the current working directory.
- For network scripts, if the full path of the script is not specified, `rosh` uses the search path indicated by the `NETWORK_SCRIPT_PATH` environment variable. If this variable is not set, `rosh` searches for the script in these directories:

```
/opsw/Script/Network/Command/  
/opsw/Script/Network/Diagnostic/  
/opsw/Script/Network/Advanced/
```


rosh Operations

The `rosh` command establishes a client connection which enables you to remotely run programs on managed servers. The Opsware Global Shell feature provides the following modes of operation for `rosh`:

- **jump**: This operation starts a shell session in a pseudo-terminal on a managed server. This mode operates when you do not use the `-s` option and when you do not specify a command or a script. You must have the `loginToServer` permission on the managed server to jump.
- **reach**: This is a remote execution of commands that are native to the platform (operating system) of the managed server. This mode operates when you specify a command. You must have the `runCommandOnServer` permission on the managed server to reach.
- **push**: This is a remote execution of a script on a managed server. The script is stored in the OGFS and is sent to the managed server by `rosh`. You must have the `runCommandOnServer` permission on the managed server.

rosh Examples

The following examples illustrate what these operations look like for an Opsware user named `psi` at this path:

```
/opsw/Server/~/salish.snv1.corp.opsware.com/files/root/etc
```

```
[psi@m168 etc] (538) $ uname -n; id; pwd
m168.dev.opsware.com
uid=59796(psi) gid=59796(psi) groups=59796(psi)
/opsw/Server/~/salish.snv1.corp.opsware.com/files/root/etc
```

The `rosh jump` command would display the following information about the managed server:

```
[psi@m168 etc] (539) $ rosh
[root@salish etc]# uname -n; id; pwd
salish.snv1.corp.opsware.com
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),
,12(mail),7(lp),4(adm),9(kmem),6(disk),5(tty),3(sys),2(daemon),
8(mem)
/etc
[root@salish etc]# logout
```

The `rosh reach` command displays the following information about the managed server:

```
[psi@m168 etc] (541) $ rosh "uname -n; id; pwd"
salish.snv1.corp.opsware.com
uid=0 (root) gid=0 (root)
groups=0 (root) , 1 (bin) , 2 (daemon) , 3 (sys) , 4 (adm) , 6 (disk) , 10 (wheel)
, 12 (mail) , 7 (lp) , 4 (adm) , 9 (kmem) , 6 (disk) , 5 (tty) , 3 (sys) , 2 (daemon) ,
8 (mem)
/etc
```

The `rosh` push command displays the following information about the managed server:

```
[psi@m168 etc] (544) $ cat /tmp/who.sh
#!/bin/sh
uname -n
id
pwd
```

```
[psi@m168 etc] (543) $ rosh -s /tmp/who.sh
salish.snv1.corp.opsware.com
uid=0 (root) gid=0 (root)
groups=0 (root) , 1 (bin) , 2 (daemon) , 3 (sys) , 4 (adm) , 6 (disk) , 10 (wheel)
, 12 (mail) , 7 (lp) , 4 (adm) , 9 (kmem) , 6 (disk) , 5 (tty) , 3 (sys) , 2 (daemon) ,
8 (mem)
/etc
```

The following example runs a script on a network device:

```
$ cd /opsw/Network/@/sw-ee-1-2b
$ rosh -s -C 'Updating device location' \
-V 'Location=Opsware - Sunnyvale' 'Set Location'
run script task 8725081 completed successfully.
Results:
Script 'Set Location for Cisco IOS configuration (for drivers:
Cisco switches, Catalyst 2950, 3550, 3750 & 8500 series, IOS
version 12.x)' completed.
```

swenc Utility

The `swenc` command enables you to switch the character encoding within a Global Shell session.

swenc Syntax

The `swenc` command has the following syntax:

```
swenc [-e encoding] [-T {on | off}] [-E] [-x] [-c command]
```

Table C-4 describes the `swenc` options.

Table C-4: `swenc` Options

OPTION	DESCRIPTION
<code>-c <i>command</i></code>	Executes <i>command</i> and exits, reverting the session encoding to its previous state.
<code>-E</code>	Lists the valid character encodings.
<code>-e <i>encoding</i></code>	Changes the character encoding of the current session.
<code>-T {on off}</code>	Turns on or off the transcoding of data from the Unix managed server. (Data from Windows servers does not need to be transcoded.) See “Transcoded Data in a Managed Server” on page 394.
<code>-x</code>	Prevents the launching of a sub-shell.

swenc Usage Rules

The following usage rules apply to the `swenc` utility:

- If you specify no options, `swenc` displays the character encoding and transcoding mode of the current session.
- Unless you specify the `-x` option, `swenc` starts a new sub-shell, which uses the encoding specified with the `-e` option. To leave the sub-shell and revert to the previous encoding, enter `exit`.
- Changing the encoding with `swenc` affects all processes in the current session, including background processes. If you change the encoding while background processes are running, the background processes might encounter errors.
- The `swenc` command affects only the current Global Shell session. For example, if you run the `rosh` command after the `swenc -e` command, the `rosh` command does not inherit the encoding that you changed with the `swenc` command.
- The `swenc` command does not change the working directory of the session, unless the working directory contains path names that cannot be represented in the new encoding. In this case, the working directory is the user’s home directory.

- If you change the character encoding, make sure that the encoding of the terminal application that hosts the Global Shell and Remote Terminal sessions is set properly. To view or change the terminal client, go to the Terminal and Shell Preferences of the Opware SAS Client.

Appendix D: OGFS Directories

IN THIS APPENDIX

This section discusses the following topics:

- Directories in the OGFS
- root (/) Directory
- /opsw Directory
- /opsw/Server Directory
- Other Directories Under /opsw
- Network Directories

Directories in the OGFS

The Opsware Global File System (OGFS) is accessible from within a Global Shell session.

Many directories contain similar files. The `id` file contains the Opsware SAS unique identifier (primary key) for the object represented by the directory. The `attr` directory contains text files that describe the attributes of the managed server. The `info` file is deprecated in Opsware SAS 6. Instead of the `info` file, use the files in the `attr` directory. The `self` file represents this specific server object (instance). The `method` directory contains executables that invoke the methods in the Opsware API. For details on the executables in the `method` directory, see the *Opsware® Automation Platform Developer's Guide*.

In the directory listings that follow, the italicized text represents variable paths (specific instances of objects in the data model). For example, *server-1* is the name of a specific managed server. The italicized text in parentheses contains comments.

root (/) Directory

At the `root` level of the OGFS is a directory for each Opware user. Each user directory and all files and directories under it are visible only to processes in an authenticated session.

Each Opware user has the following private directories:

- A home directory which is at `/home/user-name` (Opware user name)
- Temporary directories located at `/tmp`, `/var/tmp` and `/usr/tmp`

Each user's home directory contains a `public` directory (`/home/user-name/public`) which is readable by all other Opware users and can be used to share files with other Opware users.

The `root` directory has the following structure:

```
/. (root)
  bin/
  dev/
  etc/
  home/
  lc/
  lib/
  opsw/
  opt/
  proc/
  sys/
  tmp/
  usr/
  var/
```

/opsw Directory

The `opsw` directory represents the data model of Opware SAS. For example, the `/opsw/Customer` directory represents customer objects in the data model. Global Shell scripts and other client applications can navigate within the data model in the OGFS. Except for the `api` and `bin` directories, all of the directories under the `opsw` directory represent objects. The `api` directory contains executables that invoke methods on the Opware SAS API. The `bin` directory contains Global Shell utilities such as `rosh` and `aaa`.

For Opware SAS, the top level of the `opsw` directory has the following structure:

```

/opsw/
  api/
  Application/
  .Application.ID/
  bin/
  Customer/
  .Customer.ID/
  Facility/
  .Facility.ID/
  Group/
  .Group.ID/
  Hardware/
  .Hardware.ID/
  Library/
  .Library.ID/
  NetModel/
  NetOS/
  NetType/
  Network/
  .Network.ID/
  OS/
  .OS.ID/
  Realm/
  .Realm.ID/
  Script/
  Server/
  .Server.ID/
  ServiceLevel/
  .ServiceLevel.ID/

```

The ID directories organize objects by their unique Opsware identifier. These directories are equivalent to those organized by name. For example, if a server with an ID 10043 is named `m44.opsware.com`, then the following directories contain the same information:

```

/opsw/.Server.ID/10043
/opsw/Server/@/m44.opsware.com

```

If the Opsware NAS is installed, the `/opsw` directory also contains several network directories. See “Network Directories” on page 577.

/opsw/Server Directory

The `Server` directory not only contains information about managed servers, but also organizes the servers by their associated objects. For example, the `/opsw/Server/@Group` directory organizes servers by device group.

At the top level, the `/opsw/Server` directory has the following structure:

```

/opsw/Server/
  @/
    server-1/
    server-2/
    . . .
  @Application/
    Application Servers/
    Database Servers/
    . . .
  @Customer/
    customer-1/
    customer-2/
    . . .
  @Facility/
    facility-1/
    facility-2/
    . . .
  @Group/
    Private/
      private-group-1/
      private-group-2/
      . . .
    Public/
      public-group-1/
      public-group-2/
      . . .
  @Hardware/
  @OS/
  @ServiceLevel/

```

The sections that follow list some of the directory structures under `/opsw/Server`.

`/opsw/Server/@` Directory

This directory contains all managed servers. The `files` directory reflects the file system of the managed server. When you modify the file system beneath the `files` directory, you do so as a specific user (such as `login-1`) of the managed server.

The `Interface` directory contains information about the network interface of the server. This directory might contain symbolic links to a network device. See “`/opsw/Network Directory`” on page 578 for more information on these links.

The paths in the following directory structure are under `/opsw/Server/@`. For example, the full path name of `server-1` in the following structure is

```
/opsw/Server/@/server-1/.
```



```
server-1/
  attr
  ChangeLog
  complus
  CPU/
    0
    1
    . . .
  CustAttr/
    custom-attribute-1
    custom-attribute-2/
    . . .
  files/
    login-1/
      (file system as seen by login-1)
    login-2/
      (file system as seen by login-2)
    . . .
  info
  Interface/
    network-interface-1/
    . . .
  Memory/
    RAM
    SWAP
  metabase/
    login-1/
      (metabase as seen by login-1)
    login-2/
      (metabase as seen by login-2)
    . . .
  method/
  registry/
    login-1/
      (registry as seen by login-1)
    login-2/
      (registry as seen by login-2)
    . . .
  self
  Storage/
    storage-device-1/
    . . .
server-2/
  . . .
server-3/
  . . .
```

/opsw/Server/@Facility Directory

This directory filters servers according to their facility:

```

facility-1/
  @/ (all servers in facility-1)
    server-1/
    server-2/
    . . .
  @Group/
    group-1/
      @/ (all servers in both facility-1 and group-1)
        server-1/
        . . .
    group-2/
    . . .
facility-2/
. . .

```

/opsw/Server/@Group Directory

This directory does not contain network devices. This directory filters servers according to their device groups:

```

group-1/
  @/ (all servers in group-1)
    server-1/
    . . .
  child-group-1/
    @ (all servers in child-group-1)
      server-1/
      . . .
  child-group-2/
  . . .
  @Facility/
    facility-1/
      @ (all servers in both group-1 and facility-1)
        server-1/
        . . .
group-2/
  @/ (all servers in group-2)
  . . .

```

/opsw/Library Directory

The `Library` directory contains information about folders and the objects within folders: application policies, OS sequences, and packages. This directory has the following structure:

```

/opsw/folder-path-1/@/
    AppPolicy/
        app-policy-1/
            attr/
            method/
            self
        app-policy-2/
        . . .
    attr/
    method/
    OSSequence/
        os-sequence-1/
            attr/
            method/
            self
        os-sequence-2/
        . . .
    Package/
        package-1/
            attr/
            method/
            self
        package-2/
        . . .
    self
/opsw/folder-path-2/
. . .

```

Other Directories Under /opsw

This section lists, in alphabetical order, the object directories under `/opsw` other than the `Server`, `Library`, and `Net*` (network) directories.

/opsw/Application Directory

This directory is deprecated in Opsware SAS 6.0.

This directory represents the Opsware Software Tree, a hierarchical structure for organizing applications:

```

/opsw/Application/
    Application Servers/
        application-1/
            @/
                CustAttr/
                    custom-attribute-1
                    custom-attribute-2
                    . . .
                .id
                info
                child-application-1/
                    @/
                        . . .
                        grandchild-application-1/
                            @/
                                . . .
                                grandchild-application-2/
                                    . . .
                                    child-application-2/
                                        . . .
                                        application-2/
                                            . . .
    Database Servers/
        application-1/
            . . .
    Operating System Extras/
        application-1/
            . . .
    Other Applications/
        application-1/
            . . .
    System Utilities/
        application-1/
            . . .
    Web Servers/
        application-1/
            . . .

```

/opsw/Facility Directory

Typically, a facility identifies the geographical location of a data center, such as a city or building. This directory contains information about facilities and the servers they manage:

```

/opsw/Facility/
    facility-1/
        @/
            attr

```

```

    CustAttr/
        custom-attribute-1
        custom-attribute-2
        . . .
    info
    method
    self
    Server/
        server-1/
        server-2/
        . . .
    facility-2/
    . . .

```

/opsw/Group Directory

This directory represents device groups. This directory also contains groups for network devices under the following conditions:

- Opsware NAS is installed.
- The Opsware SAS group has the NAS-associated attribute set.
- The SAS and NAS group names are the same.

In the following structure, the `child-group` and `grandchild-group` reflect nested device groups:

```

/opsw/Group/
    Public/
        group-1/
            @/
                CustAttr/
                    custom-attribute-1
                    custom-attribute-2
                    . . .
                info
                Server
                    server-1/
                    server-2/
                    . . .
                child-group-1/
                    @/
                        . . .
                        grandchild-group-1/
                            @/
                                . . .
                                grandchild-group-2/

```

```

        . . .
        child-group-2/
        . . .
        group-2/
        . . .
Private/
        group-1/
        . . .
        group-2/
        . . .

```

/opsw/Library

This directory corresponds to the Library of folders displayed by the SAS Client.

```

/opsw/Library/ct
        folder-1/
        @/
            attr
            method
            OSSequence
            self
            Software
            SoftwarePolicy
        subfolder-1/
        @/
            . . .
        subfolder-2/
        . . .
        folder-2/
        @/
            . . .

```

/opsw/OS Directory

This directory contains information about the operating systems defined in Opware SAS. It does not contain the actual bits for the operating systems, which are stored in the OS Provisioning Media Server. The /opsw/OS directory has the following structure:

```

/opsw/OS/
        os-name-1/
        Not Assigned/
        @/
            CustAttr/
                custom-attribute-1
                custom-attribute-2
                . . .

```

```

    info
    Serv-1/er
        server-1/
        server-2/
        . . .
    os-name-2/
    . . .

```

/opsw/Permissions Directory

This directory contains information about the Global Shell permissions. The `info` directory contains a file for each operation (permission) that can be granted with the `aaa` utility. For each user group, the `operations` subdirectory contains a text file corresponding to an operation (such as `launchGlobalShell`) that have been granted to the group by `aaa`. The contents of these text files summarize the parameters of the permissions for that operation and user group.

For example, the `readServerFilesystem` text file is in the `operations` directory of the `Advanced Users` group:

```

/opsw/Permissions/UserGroups/Advanced Users/operations/
readServerFilesystem

```

The `readServerFilesystem` text file contains the following information:

```

Facility: C40(40) Login: sysadmin
Group: Unix Servers (2880040) Login: root

```

In this example, all members of the `Advanced Users` group can read the file system as user `sysadmin` on servers that belong to `Facility C40` (with ID 40), and as user `root` on servers that belong to the device group `Unix Servers` (with ID 2880040).

If a user group directory does not contain a text file for an operation, then the group does not have permission to perform that operation. If the text file is empty, the user group has permission to perform the operation, but the operation has no parameters. The `launchGlobalShell` operation, for example, has no parameters.

The `/opsw/Permissions` directory has the following structure:

```

/opsw/Permissions/
    info/
        launchGlobalShell
        loginToServer
        readServerComplus
        readServerFilesystem
        readServerMetabase
        readServerRegistry

```

```

relayRdpToServer
runCommandOnServer
runTrustedOnServer
writeServerFilesystem
UserGroups/
    user-group-1/
        description
        operations/
            launchGlobalShell
            loginToServer
            . . .
    user-group-2/
        . . .

```

/opsw/Realm Directory

A realm is a logical name for a group of IP addresses that can be contacted by a particular set of Opware Gateways. Typically, each Satellite and Facility has one or more distinct realms. To find out which managed servers belong to a realm, note the server names below the `realm/@/Server` subdirectory.

The Realm directory has the following structure:

```

/opsw/Realm/
    realm-1/
        @/
            info
            Server/
                server-1/
                server-2/
                . . .
    realm-2/
        . . .

```

/opsw/Script/Shared Directory

This directory contains utility scripts that are included with Opware SAS. These scripts are not the same as the DSE shared scripts that are accessible with the SAS Web Client. The contents of this directory cannot be changed by end users.

```

/opsw/Script/
    Shared/
        script-1/
            description
            policy
            source
            version

```



```
script-2/
```

```
. . .
```

/opsw/ServiceLevel Directory

This directory is deprecated in Opware SAS 6.0.

Service levels are user-defined categories such as Silver, Gold, and Platinum. The /opsw/ServiceLevel directory has the following structure:

```
/opsw/ServiceLevel/
  service-level-1/
    @/
      CustAttr/
        custom-attribute-1
        custom-attribute-2
        . . .
      .id
      inf-1/o
      . . .
      child-service-level-1/
        @/
          . . .
          grandchild-service-level-1/
            @/
              . . .
            child-service-level-2/
              . . .
          Server/
            @/
              . . .
          service-level-2/
            . . .
```

Network Directories

For Opware NAS, the top level of the opsw directory includes the following subdirectories:

```
/opsw/
  . . .
  NetModel/
  NetOS/
  NetType/
  Network/
  .Network.ID/
```

```

. . .
Script/Network

```

/opsw/Network Directory

This directory organizes the devices by their model, OS, type, and group. All network devices are in the `/opsw/Network/@` directory. The `ChangeLog` directory contains time-stamped events for the device. The `Config` directory contains time-stamped configuration files.

At the top level, the `/opsw/Network` directory has the following structure:

```

/opsw/Network/
    @/
        device-1/
            attr/
            ChangeLog/
            Config/
            info
            method/
            Module/
            Port/
                port-1/
                    .id
                    info
                    Link/
                port-2/
                    . . .
            self
            Vlan/
        device-2/
            . . .
    @Group/
    @NetModel/
    @NetOS/
    @NetType/

```

The `Port` and `VLAN` directories contain Layer 2 information. Within each subdirectory of the `Port` directory, an `info` file contains duplex information and other data for a specific network port. The `Link` directory contains a symbolic link to a server interface or a port on another network device (if the MAC address to the interface or port is available). In the following example, the `eth0` under `Network` is a symbolic link to `eth0` under `Server`:

```

/opsw/Network/@/sw-ee-1-2b/Port/FastEthernet0_1/Link/eth0
    symbolic link to -->
/opsw/Server/@/m180.mycomp.com/Interface/eth0

```

Similarly, the Server directory can have a symbolic link to the corresponding entry under Network:

```
/opsw/Server/@/x.mycomp.com/Interface/eth0/Link/FastEthernet0_7
    symbolic link to -->
/opsw/Network/@/sw-ee-2-4a/Port/FastEthernet0_7/eth0
```

/opsw/Network/@Group Directory

This directory does not contain groups for managed servers. This directory filters network devices according to their groups:

```
group-1/
  @/ (all devices in group-1)
    device-1/
      . . .
    @NetModel/
    @NetOS/
    @NetType/
  child-group-1/
    @ (all devices in child-group-1)
      device-1/
        . . .
  child-group-2/
    . . .
group-2/
  @/ (all devices in group-2)
  . . .
```

/opsw/NetModel Directory

This directory contains subdirectories for vendors, for example, /opsw/NetModel/Cisco. The /opsw/NetModel directory has the following structure:

```
vendor-1/
  model-1/
    @/
    @Group/
    @NetOS/
    @NetType/
  model-2/
  . . .
vendor-2/
. . .
```

/opsw/NetOS Directory

This directory organizes devices by their operating system. The /opsw/NetModel directory has the following structure:

```
family-1/  
  os-1/  
    @/  
    @Group/  
    @NetOS/  
    @NetType/  
  os-2/  
  . . .  
. . .  
family-2/  
. .
```

/opsw/NetType Directory

This directory organizes network devices by the following types:

```
Firewall  
L3Switch  
L4to7Switch  
Proxy  
Router  
Switch  
unknown  
VPN  
Wireless Access Point  
WirelessAP
```

The /opsw/NetType directory has the following structure:

```
type-1/  
  
  @/  
  @Group/  
  @NetOS/  
  @NetType/  
type-2/  
. . .
```

/opsw/Script/Network Directory

This directory contains utility scripts for network devices. For information about these scripts, see the Opsware NAS documentation.

```
/opsw/Script/Network/
```

Advanced/
Command/
Diagnostic/

Appendix E: Glossary

IN THIS APPENDIX

This appendix describes terminology and acronyms used in Opsware SAS.

ACM See Application Configuration Management.

Ad-Hoc scripts A script that is created (or uploaded) and then immediately executed by a user. The script is intended for one-time use and is not stored in Opsware SAS.

administrator See Opsware administrator.

Agent See Opsware Agent.

Agent Installer An application that installs the Opsware Agent on a server.

Agent Uninstaller An application that uninstalls the Opsware Agent on a server.

application A set of tiers and sub-tiers, such as a Web tier running Apache on Linux, an application tier running WebLogic on Windows, and a database tier running Oracle on Solaris.

application component An object that represents a process of running software, such as Apache, Oracle, BEA WebLogic, Microsoft® SQL Server, and so on.

application configuration Contains application configuration templates associated with an application.

Application Configuration Management (ACM) An Opsware feature that enables you to manage and modify configuration files for applications on managed servers.

application definition Specifies an application's logical construction in terms of tiers, subtiers and the application components contained in those tiers. Allows you to transform a data display that contains extraneous and hard-to-understand information into a focused and easy-to-understand view of the data that is relevant to the application of interest.

application tier A set of process families that you create to organize the Application View so that you can see a compelling diagram of multiple servers, the connections among them, clients connecting to them, and dependencies to which they connect.

audit A set of rules that express the desired state of a managed server's configuration objects – for example, a server's file system directory structure or files, a server's Windows Registry, application configuration, and so on.

audit job The process that performs an audit.

audit policy A collection of rules that define a desired state of configuration for a server.

audit result The results of running an audit, which will show how a target server or groups of servers's configuration object values match or mismatch the values.

Automated Configuration Tracking An Opware feature that allows users to monitor critical configuration files and configuration databases. When Opware SAS detects a change in a tracked configuration file or configuration database, the system can perform a number of actions, including backing up the configuration file or sending an email to a designated individual or group.

available patch A patch that the patch administrator has tested and marked as available. Only patches that have been marked as available can be installed by anyone other than a patch administrator. (The patch administrator can install an unavailable patch in order to test it.)

available server A reserve of new, unconfigured Opware-enabled servers ready for quick deployment. The provisioned server can be moved into the Live environment to replace existing servers, add capacity, or support new applications. While optional, this provides faster recovery options in cases of hardware failure.

backup A feature in Automated Configuration Tracking that performs a backup of a file or database when it detects a change to a tracked configuration file or database. This action is performed only if the backup action is selected in the configuration tracking policy for the file or database.

backup (CDR) The process of saving the entire contents of the current Live directory for a specific service to the Backup directory. Code Deployment & Rollback (CDR) saves the backup copy to the local disk for the host on which the Backup operation was run. Only one backup copy is maintained at any time for a service.

backup event An event that causes configuration files or configuration databases to be backed up. Types of backup events include manual, full, and triggered.

Boot Server A part of the OS Provisioning feature that supports network booting of Sun and x86 systems with inetboot and PXE, respectively. The processes used to provide this support include the Internet Software Consortium DHCP server, and Sun Solaris TFTP and NFS.

Build Manager A part of the OS Provisioning feature that facilitates communication between the OS Boot Agent and the Command Engine for OS provisioning.

CDR See Code Deployment & Rollback (CDR).

change log An audit trail of changes made to a node (read-only). The log identifies who has recently modified the node and who has added or removed software packages, operating systems, and servers. It also tracks who has created or removed subordinate nodes.

Code Deployment & Rollback (CDR) An Opsware feature used to push updated code and content to staging host servers.

Code Deployment Role A specific role that authorizes access to capabilities and functions with the Opsware Code Deployment & Rollback feature.

combined event history log A record of events performed on servers and network devices in your environment. These events are recorded in detail as actions performed on a certain date, by a certain user, on a certain server, or on a certain network device.

Command Engine The Opsware SAS component that enables distributed programs to run across many servers. The Command Engine handles the entry of scripts into the Opsware Model Repository (the script storage location in Opsware SAS) and the versioning of stored scripts. Command Engine scripts are written in Python and run on the Command Engine server.

Communication Test A feature that helps in identifying managed servers with unreachable Opsware Agents. A Communication Test lists all servers with unreachable agents, returns specific errors associated with each unreachable agent, and provides troubleshooting information to resolve the error. To determine if an Opsware Agent is reachable, the Communication Test runs the Command Engine to Agent Communication, Crypto Match, Agent to Command Engine Communication, Agent to Data Access Engine, Agent to Software Repository Communication, and Machine ID mismatch.

compliance The degree to which a server object conforms to a test.

configuration template A set of values that represent the configuration file of an application.

configuration tracking policy The configuration tracking policy defines the set of files or configuration databases to be monitored, and the actions to be taken when change is detected to a tracked file.

configuration tracking reconcile The process by which new configuration tracking polices or changes to existing configuration tracking polices are deployed on servers.

core See Opsware core.

custom attributes Attributes such as miscellaneous parameters and named data values that users can set for servers. This is used when performing a variety of Opsware

functions, including network and server configuration, notifications, and CRON script configurations.

custom extension Developed and deployed by Opware Inc. support representatives, a custom extension is a Command Engine script that extends Opware SAS functionality. A custom extension is often tailored to meet the specific needs of a customer.

customer An account within Opware SAS that has access to designated resources, such as servers and software.

cutover A feature in CDR, that causes the Update directory and current Live directory to be identical. The different files from the Update directory are automatically synchronized with the current Live directory.

Data Access Engine The XML-RPC interface to the Model Repository that simplifies interaction with various clients such as the SAS Web Client, system data collection, and monitoring agents on servers.

data center Legacy term. See facility.

data link connection A layer 2 connection that includes switches that are directly connected to a managed server and switches that are indirectly connected through other switches.

DCML Exchange Utility (DET) A command-line tool (cbt) for importing and exporting Opware SAS content. The primary function of this tool is to inject a newly-installed Opware core with content from an existing core.

deactivated server A server removed from Opware management even though its history still exists.

deployment Within CDR, automatically pushes code and content from a staging server to a live network server.

deprecated A possible state of a package or patch in Opware SAS. A deprecated package or patch can no longer be installed on a managed server, but might still be installed on a server before the patch or package was deprecated.

device A managed server or network device.

device group In SAS, a device group can contain managed servers and network devices, or only managed servers. In NAS, a device group contains only network devices. A device group helps you categorize your devices (servers and network devices) in ways that make sense for your organization.

Distributed Scripts An Opware feature that allows you to manage scripts in your managed environment.

Dormant Opsware Agent An Opsware Agent that runs in the dormant mode after its installation when the Opsware SAS core is not available on the network. The dormant agent periodically attempts to contact the core and when the core is available, it performs the initialization tasks to complete its installation.

duplex mismatch A configuration mismatch between the speed and duplex of a managed server and a connected network device.

dynamic group A server group that contains servers added to or removed from the group based on a set of user-defined rules.

email notification list An the Automated Configuration Tracking feature that sends an email to those listed in an email notification list whenever a change to a tracked file or configuration database is detected.

Environment Tree The Environment Tree manages characteristics about a customer's unique data center environment, including hardware, location of servers, network infrastructure, application names, business units, and service levels assigned to servers and applications. The information contained in the Environment Tree, combined with the information contained in the software policy, is used by the Opsware Automation Platform to model and simulate operational changes before they are executed in the production environment.

facility The collection of servers that a single Opsware core manages. A facility can be all or part of a data center, server room, or computer lab.

folder A hierarchal file-system type organization structure that allows you to organize and manage your software resources and allows you to define security boundaries to control access to its content across user groups.

full backup During a full backup, all tracked configuration files that were selected to be backed up are backed up (and not just the files that have changed). Full backup is performed if you select backup as the action for a tracked configuration file.

gateway See Opsware Gateway.

Global Shell A Unix shell that accesses the Opsware Global File System (OGFS) and managed servers in a secure environment.

group See device group.

Health Check Monitor (HCM) The command-line scripts that check the status of Opsware SAS core components.

IDK Intelligent Software Module (ISM) Development Kit. The command-line tools (primarily ismtool) that build and upload ISMs into Opsware SAS.

Import Media tool A utility script included with Opware SAS that is used to import OS media from the Media Server to Opware SAS.

inclusions/exclusions criteria Specifies how to include and exclude directories and files during the snapshot or audit process.

incremental backup During an incremental backup, only targets that have changed since the last backup (and that have been selected to be backed up) are backed up. Incremental backup is performed if you select backup as the action for a tracked configuration file.

initialization Legacy term. See OS Provisioning.

IP Range Groups A designated set of servers assigned to a customer account, grouped by either a physical or a logical list.

IP Ranges A designated grouping of servers.

ISM Intelligent Software Module. A set of file and directories that include application bits, installation scripts, and control scripts for applications that are to be installed on managed servers.

ISM control A script within an ISM package that can be run on a managed server.

job Any major process run by the SAS Web Client or the SAS Client such as a communication test or a software installation.

layer 2 connection See data link connection.

Library In the SAS Client, the Library provides a way to display features such as application configurations, software policies, patches, patch policies, packages, OS sequences, and OS profiles managed by Opware.

Live directory In CDR, the directory that stores the actual code and content required to run a live site.

MAC See Media Access Control Address (MAC).

Machine ID (MID) A unique identifier that Opware SAS uses to identify the server. Opware SAS assigns a unique number to the server when it first registers and stores the Machine ID and uses it to identify each server.

managed server A server that has an Opware Agent installed on it and is under the control of a particular Opware core.

management IP The IP address that Opware SAS uses to communicate with the Opware Agent on the server.

manifest Within CDR, a list of files that preview the results of an update to be performed. Each entry in the list specifies the file size, the last-modified date, the time stamp, and the full directory path to the listed file.

Media Access Control Address (MAC) The network interface card's unique hardware number. The MAC is used as the server's physical address on the network.

Media Resource Locator (MRL) A network path in URL format that is registered with Opware SAS. The path defines the installation media for an OS.

Media Server Contains the vendor-supplied OS media used during OS provisioning over the network. The OS media on the Media Server is accessed over the network by using NFS for Linux and Solaris OS provisioning, and by using SMB for Windows OS provisioning.

MID See Machine ID.

Model Repository The Opware database that stores information about managed server configurations within Opware SAS. It contains all information necessary to build, operate, and maintain an Opware-managed site. It includes data on all managed servers, the hardware associated with those servers, their memory, CPUs, storage capacity, configuration, IP addresses, DNS configuration, and so on.

Model Repository Multimaster Component The application that propagates and synchronizes changes from each Model Repository database to all other Model Repository databases.

Modeling and Change Simulation Engine Opware SAS enables users to first model and simulate proposed operational changes to their environment before propagating these changes to production servers and applications. Using the information contained in the Software and Environment Trees, the Modeling and Change Simulation Engine maintains a model of the various hardware and software configurations and other customer characteristics associated with each of the production servers under Opware SAS control.

MRL See Media Resource Locator (MRL).

multimaster core An Opware core that belongs to a multimaster mesh.

multimaster infrastructure component See Model Repository Multimaster Component.

multimaster mesh A set of two or more Opware cores that are linked by synchronizing the data in the Model Repositories at each of the cores. The Model Repositories in each

of the cores are continually updated so that they are exact duplicates of each other. All the Opware cores in a multimaster mesh can be managed through a single SAS Web Client.

My Jobs A page in the SAS Web Client that displays a list of jobs from the Model Repository such as software installation or server provisioning.

My Scripts Private scripts that can only be executed by the user who created the script. My Scripts are created for personal use.

name-value pairs Legacy term. See custom attributes.

NAS Integration An Opware feature that enables you to closely examine detailed information about managed servers and the network devices connected to them so that you can determine how they are related and then, subsequently, coordinate and implement those changes.

OCLI See Opware command Line Interface (OCLI).

OGFS See Opware Global File System.

Opware administrator The person responsible for overall administration, policy, and practices for accessing Opware SAS. The administrator can add users, define access to specific Opware SAS features, allow users to view site information, and deploy new code and content to their site.

Opware Agent Intelligent software on Opware-managed servers that is used to make changes to the servers. Depending on the request, the agent might use Global Opware services. Some functions supported include software installation and removal, software and hardware configuration, server status reporting, and auditing.

Opware API An API that accesses the functionality and data model of Opware SAS. The Opware API supports Web Services, Java RMI, and other types of clients. The Opware API enables you to extend, integrate, and customize Opware SAS.

Opware Automation features Opware SAS is made up of a set of Opware Automation features. Opware Automation features are the components that automate particular IT processes. The Opware Automation features include the following functions: Configuration Tracking, Code Deployment and Rollback, Script Execution, and Data Center Intelligence Reporting.

Opware Automation Platform The Opware API and runtime environment that facilitate the integration and extension of Opware SAS. The Opware APIs expose core services such as audit compliance, Windows patch management, and OS provisioning. The runtime environment (hub) executes scripts that can access the Opware Global File System (OGFS).

Opware Discovery and Agent Deployment A feature that helps deploy Opware Agents to a large number of servers through the SAS Client.

Opware SAS Web Client A web-based user interface for managing the Opware environment.

Opware Command Line Interface (OCLI) OCLI 1.0 has two commands, upload and download, which import and export files between the local file system and the Software Repository. OCLI 2.0 is intended for use only by Opware Inc. support representatives.

Opware core The server side of Opware SAS server-agent architecture. A core consists of the Opware components (such as the Model Repository, the Software Repository, the Data Access Engine, and the Command Engine) for a particular installation.

Opware Gateway Provides connectivity with an Opware core either directly or through a network of gateways. All traffic between the servers in the Satellite and the core that manages them is routed through Opware Gateways.

Opware Global File System (OGFS) The Opware Global File System is a single, unified file system view of all file systems for all managed servers in Opware SAS.

Opware installation Either a standalone core, multimaster core, or Opware Satellite.

Opware model space The Opware Global File System (OGFS) structure that is derived from the Model Repository.

Opware Satellite Installed in a remote facility, an Opware satellite provides a network connection and bandwidth management for a core that manages remote servers. A Satellite must be linked to at least one core, which may be either standalone or multimaster.

Opware SAS The server management application that preserves the knowledge of system administrators, network engineers, and database administrators in a centralized knowledgebase. It automates previously manual tasks associated with the deployment, support, and the growth of a data center infrastructure.

OS Build Agent A part of the OS Provisioning feature that is responsible for registering bare metal servers in Opware SAS and guiding the installation process.

OS media Installation software for an OS from the software vendor that is distributed on a CD-ROM, or DVD, or can be obtained by downloading the software from the vendor's FTP site.

OS Provisioning The process of installing a basic set of software components, including an operating system and an Opware Agent. After provisioning is complete, the server is ready to be managed by Opware SAS.

Package Repository Legacy term. See Software Repository.

package A collection of executables, configuration, or script files that are associated with an Opware-installable application or program. In Opware SAS, a package contains software package files registered in the Software Repository and software for operating systems, applications (for example, BEA WebLogic, IBM WebSphere), databases, customer code, and software configuration information.

packaging server A managed server that has the IDK installed on it. Visual Packager requires a packaging server for each type of operating system for the packages you plan to create.

patch A piece of object code (binaries) that is inserted into (patched into) an executable program to temporarily fix a known defect.

patch management administrator Administrator responsible for testing patches and defining patch options, such as installation and uninstallation scripts. A patch cannot be installed by other personnel until the patch administrator has marked the patch available through the SAS Web Client.

Patch Management An Opware feature that allows you to upload, test, and deploy patches in a safer and uniform way.

permission A setting within a User Group that allows or disallows access to Opware SAS features and resources. A resource is usually a set of managed servers. The set of managed servers corresponds to a facility, customer, or server group. A feature is an action, such as provisioning an OS.

physical connection The connection inferred from data link connections and represents direct connections (cables) between server and switches.

platform The name and version of an operating system.

post-install script A shell script invoked on a managed server immediately after a software package is installed on a managed server.

post-uninstall script A shell script invoked on a managed server immediately after a software package is removed from the managed server.

pre-install script A shell script invoked on a managed server immediately before a software package is installed on a managed server.

pre-uninstall script A shell script invoked on a managed server immediately before a software package is removed from the managed server.

preview remediate Before Opware SAS installs software on a server, it performs a preview remediate, and determines what will happen when the actual remediate is

performed (for example, what packages will be installed or removed, what server reboots are required, and so forth).

primary IP A locally-configured IP address of the management interface.

private group A type of server group that can be edited, or deleted by the Opware user who created the server group.

privileges See Permissions and User Group.

public group A type of server group that can be created, edited, or deleted by any Opware user who has Manage Public Server Groups permissions.

realm One or more Opware Gateways that service the managed servers contained within an Opware realm. In Opware SAS, a realm is a routable IP address space, which is serviced by one or more gateways. All managed servers that connect to an Opware core via a gateway are identified as being in that gateway's realm.

remediate The process of updating the actual software configuration of a server based on the specified configuration stored in the Model Repository.

remediate output After a remediate operation completes, Opware SAS displays the remediate output for each server that was remediated. The remediate output aggregates output from the various installation, uninstallation, or post-installation scripts, messages from Opware SAS, and messages from the system utilities that remediate uses to perform the installation and uninstallation of packages, operating systems, and patches.

reference server A managed server that is compliant (performs as expected) and is also referred to as a known working server or a baseline server.

remote terminal A terminal window for a Unix server or an RDP client window for a Windows server.

Reports An Opware feature that enables you to create reports that provide comprehensive, real-time information about managed servers, network devices, software, patches, customers, facilities, operating systems, compliance policies, and users and security in your environment.

restore A function of the Automated Configuration feature that allows the user to return the configuration file or database to a previous state, when the backup action for a tracked file or database is selected.

restore Within CDR, the process of restoring the previous Live directory from the Backup directory to the Live directory.

restore queue The queue in which the configuration files are placed before they are restored to a server.

rollback Within CDR, returns a site to the state prior to the last cutover. During rollback, restores the set of modified and deleted files to the Live directory.

rosh The remote Opware shell is a command that makes a client connection enabling you to remotely run programs on managed servers.

Satellite See Opware Satellite

Script Execution See Distributed Scripts.

selection criteria Rules that instruct Opware SAS to collect information about server objects and how to collect that information. It optionally can also collect data for file comparison and inclusions/exclusions. Selection criteria is required for the snapshot and audit processes.

sequence The process within CDR that simplifies deployment by grouping a collection of service operations and synchronizations that can be performed as a single task.

Sequence Editor In CDR, a predefined User Group used to create, modify, or delete a sequence definition.

Sequence Performer (Production) In CDR, a predefined User Group used to directly perform or request performance of a sequence action on production hosts.

Sequence Performer (Staging) In CDR, a predefined User Group used to directly perform or request performance of a sequence action on staging hosts.

Sequence Requester (Production) In CDR, a predefined User Group used to request performance of a sequence action on production hosts.

Sequence Requester (Staging) In CDR, a predefined User Group used to request performance of a sequence action on staging hosts.

servers Any specific hardware. Specific nodes are attached to servers that determine the specific software, configuration, and other server attributes.

server assimilation Opware SAS assimilates servers that are already functioning in the operational environment, which allows users to deploy and manage new applications installed on those servers. Assimilating servers installs Opware Agents on the servers and registers them with the Model Repository.

server baselines The process of defining and provisioning servers with standard configurations. Opware templates can be used to automate the building of complete server baselines.

Server Explorer A feature of the SAS Client that allows you to browse and manage servers and server groups in your facility.

Server ID The primary key in the Opware Model Repository that represents a given server. The Server ID is used internally in Opware SAS.

server lifecycle The various server states assigned to a server by Opware SAS. Server states include Unprovisioned, Available, Installing OS, and Managed.

server management The process by which users can manage and track servers in an Opware-managed environment. Opware SAS forces changes to the operating environment by first changing the centralized configuration information in the Model Repository and then changing the actual configuration of physical servers.

Server Pool Servers that have registered their presence with Opware SAS, but do not have a full operating system installed.

server provisioning The process of installing a basic set of software components including the operating system, an Opware Agent, and other system utilities and debugging tools to manage the server. Configuration is defined in the Model Repository.

Server Search A feature that allows you to search for servers based on a variety of criteria, including OS version, installed package, customer, and installed patch.

Server Status A feature that defines server availability. The three major status conditions are USE, STAGE, and STATE.

server-based configuration tracking policy A configuration tracking policy that is defined for a particular server or group of servers, rather than for a particular software node (application).

service A host application (for example, BEA WebLogic, Allaire ColdFusion, Microsoft IIS, Apache Web Server, or iPlanet Application Server).

Service Editor In CDR, a predefined User Group used to define and modify or delete service definitions.

Service Performer (Production) In CDR, a predefined User Group used to directly perform or request performance of service operations on production hosts (servers).

Service Performer (Staging) In CDR, a predefined User Group used to directly perform or request performance of service operations on staging hosts.

Service Requester (Production) In CDR, a predefined User Group used to request performance of service operations on production hosts.

Service Requester (Staging) In CDR, a predefined User Group used to request performance of service operations on staging hosts.

service-instance Multiple independent instances of a service running on a host (for example, BEA WebLogic, which can run single or multiple instances).

Service Levels User-defined categories that are used to group servers in an arbitrary way. For example, a user can group servers by functionality, tier, application, or ontology.

Shared Scripts Public scripts that every Opware SAS user can access.

signature A set of rules that you provide and that Visual Application Manager uses to identify a process family.

Site Backup directory In CDR, the directory that stores a complete backup of the Live directory when the user issues a Backup service operation.

Site Previous directory In CDR, the directory that stores the files that have changed between the current Live directory and its previous state prior to the last cutover. It holds all the changes necessary to revert the Live directory back to the state that it was in before the last cutover.

snapshot A record of how an Opware managed server is configured at a particular point in time. Snapshots allow administrators to audit the configuration of servers and deploy files and software to correct discrepancies. A snapshot can be based on specified server objects. Server Compliance records one snapshot per server.

snapshot job The process that created a snapshot of a server or server group.

snapshot specification A definition of a target and selection criteria that will be examined during the snapshot process to capture and record information about a managed server.

software compliance Software compliance indicates whether or not the all software policies attached to the selected server are compliant with the actual server configuration.

software policy A software policy contains packages, patches, application configurations, and other software policies and allows you to install software and configure applications on managed servers simultaneously.

Software Repository The central repository for all software managed by Opware SAS. It contains software packages for operating systems, applications, databases, customer code, and software configuration information.

Software Repository Cache An Opware Satellite component that contains local copies of files. The Software Repository Cache stores files from the Software Repository of an Opware core or from another Software Repository Cache, and supplies the cached files to Opware Agents on managed servers.

Software Repository Replicator A component providing backup functionality for Software Repositories running in a multimaster mesh.

source In the snapshot process, this is the managed server that information is recorded about. In the audit process, this is an existing snapshot or server you are comparing selection criteria *from*.

standalone core An Opsware core that manages servers in a single facility. Unlike a multimaster core, a standalone core does not communicate with other cores.

static group A server group in which the servers are added to and removed from the group manually.

synchronization The process within CDR to move modified files from a directory on a source host to a directory on a destination host.

Synchronization Editor In CDR, a predefined User Group used to create, modify, or delete a synchronization definition.

Synchronization Performer In CDR, a predefined User Group used to directly perform or request performance of a synchronization action.

Synchronization Requester In (CDR), a predefined User Group used to request performance of a synchronization action.

target In the snapshot process, this is the managed server or server group you are recording information about. In the audit process, this is an existing snapshot, server, or server group you are comparing selection criteria *to*.

topology A snapshot that represents the state of a set of network devices and managed servers, the process families running on those servers, the connections among those process families, and any external clients and dependencies.

tunnel A TCP connection between two Gateways that carries multiplexed TCP or UDP connections.

Update directory The directory that CDR writes to when synchronizing modified files in source and destination hosts. After synchronization, the Update directory is different from the current Live directories. After cutover, the Update directory and current Live directory are identical.

user An individual with access to the Opsware SAS. An Opsware user belongs to one or more User Groups, which control the access of its members.

User Group Represents a role played an organization's Opsware users. The permissions specified for a user group determine what the group's members can do with Opsware SAS.

Value Set Editor Enables you to change the values in a configuration file by editing that file's value set. Each entry configuration file is represented inside the value set editor as a value set, (a key name and a value).

Visual Application Manager An Opware feature that is designed to help you understand and manage the operational architecture and behavior of distributed business applications in your IT environment.

Web Services API A SOAP-based interface that facilitates the integration of operations and business support systems with Opware SAS. The Opware Web Services API 2.2 is intended for Opware SAS 5. A different Web Services API, introduced in Opware SAS 6.1, accesses the Opware API.

Web Services Data Access Engine A web services interface to the Model Repository that provides increased performance to other Opware SAS components.

Index

A

- aaa utility553
- accessing
 - CDR440
 - Device Explorer143
 - device groups180
 - Opware SAS Web Client60
 - SAS Client75
 - SAS client options87
- ACM. See Application Configuration Management.
- adding
 - custom attributes for servers338
 - customized tracking policies470
 - server to device groups169
 - servers and server groups302
 - servers to My Servers240
 - service levels, Opware SAS Web Client to ...341
- Ad-Hoc Scripts
 - creating419
 - definition of583
 - executing419
- Agent to Command Engine (CE)
 - connection time-out500
 - DNS does not resolve501
 - gateway
 - gateway could not connect to server503
 - gateway denied access502
 - gateway time-out503
 - internal gateway error503
 - name resolution error on gateway502
 - no gateway defined502
 - no callback from agent504
 - OK499
 - old agent version501
 - realm is unreachable501
 - tunnel setup error502
- Agent to Data Access Engine (DAE)
 - connection refused505
 - connection time-out506
 - DNS does not resolve506
 - gateway
 - gateway could not connect to server508
 - gateway denied access508
 - gateway time-out509
 - internal gateway error508
 - name resolution error on gateway508
 - no gateway defined507
 - tunnel setup error507
 - OK505
 - old agent version506
 - realm is unreachable507
 - unexpected error505
 - untested505
- Agent to Software Repository (SWR)
 - connection refused510
 - connection time-out511
 - DNS does not resolve511
 - gateway
 - gateway could not connect to server514
 - gateway denied access513
 - gateway time-out514
 - internal gateway error514
 - name resolution error on gateway513
 - no gateway defined513
 - internal setup error513
 - OK510
 - realm is unreachable512
 - server identification error512
 - unexpected error510
 - untested510
- Agent. See Opware Agent.
- agent-server architecture, Opware SAS52
- Application Configuration Management
 - application configuration, definition of583
 - definition of583
 - overview50
 - value set editor
 - definition of598
- asset tracking, overview231
- audit
 - audit job, definition of584
- Audit and Remediation
 - overview47
- Audit and Remediation, browsing, Device Explorer ..

158
 audit template
 definition of584
 available
 patches, definition of584
 servers, definition of584

B

backups
 backup event, definition of584
 configuration tracking
 deleting484
 full backup466
 history search options480
 incremental backup466
 manual backup477
 restoring488
 full, definition of587
 incremental backup, definition of588
 browsers
 configuring58
 supported57
 browsing
 job logs in the SAS Client96
 Build Manager
 definition of584

C

CDR. *See* code deployment.
 change logs, definition of585
 changing
 custom field values335
 use and stage values, servers for320
 character encoding
 See encoding392
 checking
 management IP of managed server518
 network gateway configuration518
 cloning, servers323
 code deployment
 accessing440
 CDR operations previous status, viewing460
 code and content, uploading to staging437
 definition of584, 585
 deployment requests from users, processing .459
 deployment, definition of586
 features439
 live directory, definition of588
 log, accessing460

overview43
 restore, definition of593
 restoring for CDR451
 rolling back code and content451
 sequences
 definition of594
 performing457
 sequence editor, definition of594
 sequence performer, definition of594
 sequence requester, definition of594
 services
 accessing452
 overview449
 performing by hostname455
 performing by service name453
 site backup directory, definition of596
 site previous directory, definition of596
 static NAT, use with278
 synchronizations, directories, overview443
 user roles, definition of585
 Code Deployment and Rollback (CDR). *See* code deployment.
 COM+ objects
 browsing, Device Explorer157
 Command Engine to Agent (AGT)
 connection
 refused493
 time out494
 gateway
 gateway could not connect to server496
 gateway denied access496
 gateway time-out497
 internal gateway error496
 OK493
 realm is unreachable495
 request time-out494
 server not registered with Command Engine ..495
 tunnel setup error496
 unexpected error493
 untested493
 Command Engine, definition of585
 command line interface, definition of591
 Common Troubleshooting Tasks
 checking, management IP of managed server 518
 checking, network gateway configuration518
 resolving, hostname519
 restarting, an Opware agent518
 verify that agent is running516
 verify that port is open on managed sever517
 Communication Test
 about126

- creating, DCI report of 139
 - definition of 585
 - errors 128
 - exporting, unreachable server status list 139
 - running, multiple servers on 134
 - searching, unreachable servers for 137
 - types of 126
 - unexpected error 133
 - Compliance Dashboard
 - overview 47
 - components
 - Device Explorer of 143
 - configuration template
 - definition of 585
 - configuration tracking
 - backed up files, restoring 485
 - backups, definition of 584
 - definition of 584
 - email and logging actions, overview 466
 - email notification lists
 - creating 467
 - definition of 587
 - file info and file versions 483
 - manual backups 477
 - overview 43, 463
 - policies
 - definition of 585
 - overview 44
 - reconciling customized 475
 - viewing for servers 474
 - policy limits 464
 - reconcile, definition of 585
 - restore queue, definition of 593
 - restore, definition of 593
 - server-based policies, definition of 595
 - servers, customizing policies for 469
 - configuring, browsers 58
 - Connection Refused
 - Agent to Command Engine (CE) 500
 - Agent to Data Access Engine (DAE) 505
 - Agent to Software Repository (SWR) 510
 - Command Engine to Agent (AGT) 493
 - Connection Time-out
 - Agent to Command Engine (CE) 500
 - Agent to Data Access Engine (DAE) 506
 - Agent to Software Repository (SWR) 511
 - Command Engine to Agent (AGT) 494
 - conventions used in the guide 31
 - copying
 - files, Device Explorer's File System of 149
 - creating
 - Ad-Hoc Scripts 419
 - Communication Test 133
 - configuration template 150
 - configuration tracking email notification list ... 467
 - device groups for virtual servers 228
 - device groups using search 167
 - dynamic device groups 166
 - local zone 214
 - package 151
 - reports, agent installation status on 123
 - scripts 405
 - server groups 288
 - dynamic groups 291
 - static groups 288, 290
 - static device groups 165
 - Crypto Match (CRP)
 - certificate mismatch 498
 - OK 497
 - SSL negotiation failure 498
 - unexpected error 497
 - untested 497
 - custom attributes
 - adding, for servers 338
 - definition of 585
 - deleting, for servers 339
 - editing, for servers 339
 - managing, overview 337
 - overview 68
 - Custom Attributes, browsing, Device Explorer ... 158, 159
 - custom extensions
 - definition of 586
 - running 429
 - custom fields
 - changing value 335
 - customers
 - association with servers 264
 - Customer Independent, definition of 263
 - definition of 586
 - Not Assigned customer, definition of 263
 - overview 262
 - cutting over
 - code and content for CDR 447
 - definition of 586
- ## D
- Data Access Engine, definition of 586
 - Data Center Intelligence reporting
 - overview 267
 - data center. See facility.

deactivating	
servers, definition of	586
deleting	
backups for configuration tracking	484
custom attributes, for servers	339
device groups	177
files, Device Explorer's File System of	150
scripts	410, 411
servers	323
snapshot	594
deprecated packages, definition of	586
Devcie Explorer	
overview	45
Device Explorer	
accessing	143
Audit and Remediation, overview	158
compliance, overview	159
creating, configuration template	150
creating, package	151
Custom Attributes, overview	158
File System	
copying, files	149
deleting, files	150
renaming, files	150
viewing, contents	148
working with	148
installed patches, overview	157
main components	143
opening, remote terminal	144
overview	141
server properties, overview	146, 181
server summary, overview	145
services, overview	152
Software Policies, overview	152
viewing	
packages	151
server history	159
Windows IIS Metabase, overview	157
Windows Registry, overview	156
device group	362
creating	165, 166, 167
device groups	
about	161
accessing	180
adding servers	169
deleting	177
device group explorer	177
Device Groups Explorer, overview	179
duplicating	176
dynamic	164
members, overview	181
moving	175
private	164
public	163
removing servers	173
static	164
types	163
DHCP	
configuring for servers	347
directories	
live, definition of	588
site backup directory, definition of	596
synchronization for CDR, overview	443
Update directory, definition of	597
disabling, custom configuration tracking policies	473
DNS Does Not Resolve	
Agent to Command Engine (CE)	501
Agent to Data Access Engine (DAE)	506
Agent to Software Repository (SWR)	511
DNS, configuring for servers	347
domains, changing for Windows servers	348
duplicating	
device groups	176
duplicating, server groups	305
dynamic device group	164
dynamic, server groups	284
E	
editing	
custom attributes, for server	339
customized configuration tracking policies	470
scripts	408
server properties	320
service levels	342
email	
configuration tracking and logging actions	466
configuration tracking notification list, format	468
notification list attribute, search order for	468
notification lists for configuration tracking, definition of	587
enabling, custom configuration tracking policies	474
encoding	
Global Shell and Remote Terminal	94
managed server	147
multi-byte characters	397, 554
OGFS	392
script	407, 411
Terminal and RDP preferences	93
transcoding	394
viewing file contents	148
Environment Tree	

- definition of587
 - errors
 - Communication Test128
 - non-zero return codes, for scripts428
 - examples
 - Opware Agent Installer, commands & options ...
532
 - searching, ways to258
 - swapping servers' disks262
 - executing
 - Ad-Hoc Scripts419
 - My Scripts or Shared Scripts414
 - exporting
 - unreachable server list to CSV139
- F**
- facilities, definition of587
 - File System
 - copying, files149
 - deleting, files150
 - overview148
 - renaming, files150
 - viewing, contents148
 - firewall386
- G**
- Gateway Could Not Connect to Server
 - Agent to Command Engine (CE)503
 - Agent to Data Access Engine (DAE)508
 - Agent to Software Repository (SWR)514
 - Command Engine to Agent (AGT)496
 - Gateway Denied Access
 - Agent to Command Engine (CE)502
 - Agent to Data Access Engine (DAE)508
 - Agent to Software Repository (SWR)513
 - Command Engine to Agent (AGT)496
 - Gateway Time-out
 - Agent to Command Engine (CE)503
 - Agent to Data Access Engine (DAE)509
 - Agent to Software Repository (SWR)514
 - Command Engine to Agent (AGT)497
 - Global Shell
 - definition of587
 - error messages396
 - overview50, 375
 - remote Opware shell558
 - remote terminal397
 - server operations in557
 - setting, permissions553
 - groups, definition of587
- H**
- hard disks, swapping for servers262
 - histories
 - CDR operations, viewing previous status460
 - scripts, viewing versions412
 - viewing, for servers268
- I**
- icons, servers icons in the SAS Web Client .207, 311
 - IIS Metabase
 - browsing, Device Explorer156
 - import media tool, definition of588
 - installing
 - Opware Agent on unmanaged Solaris local zone
212
 - Opware Agents
 - augmenting for servers534
 - checklist for524
 - commands and options, examples532
 - definition of594
 - preparing for523
 - using CLI527
 - using ODAD116
 - verification of533
 - SAS Client72
 - Intelligent Software Module (ISM)
 - definition of588
 - Internal Gateway Error
 - Agent to Command Engine (CE)503
 - Agent to Data Access Engine (DAE)508
 - Agent to Software Repository (SWR)514
 - Command Engine to Agent (AGT)496
 - IP addresses
 - configuring for servers346
 - management IP
 - definition of275
 - viewing276
 - primary for servers, setting278
 - primary IP, definition of276
 - searching for servers by258
 - setting for servers278
 - IP range groups, definition of588
 - IP ranges
 - definition of588
 - overview345
 - ISM control, definition of588

J

jobs	
definition of	588
scheduling for servers	330
snapshot, definition of	596
time outs for	333
jump	561

L

LANG environment variable	393
LC_CTYPE environment variable	393
life cycle	
definition of	595
local attachment, definition of	588
loginToServer	561

M

Machine ID (MID), definition of	588
Machine ID Match (MID)	
MID mismatch	515
OK	515
unexpected error	515
untested	515
management IP	
definition of	275, 589
managing	
custom attributes	337
manifests, definition of	589
Media Access Control Address, definition of	589
media resource locators (MRLs), definition of	589
media server, definition of	589
Microsoft Terminal Services	93
Model Repository Multimaster Component, definition of	589
Model Repository, definition of	589
model-based approach	
servers, affects on	53
modeling and change simulation engine	
definition of	589
modeling, public server groups	284
modifying a Solaris local zone	220
moving	
device groups	175
multimaster	
mesh, definition of	589
overview of support in Opware SAS	55
multimaster core, definition of	589
My Customers, overview	63
My Jobs	

Browsing job logs in the SAS Client	96
Communication Test	139
definition of	590
overview	62
My Profile, overview	68
My Scripts, executing	414
My Servers	
overview	68
servers, adding to	240
servers, removing from	241

N

Name Resolution Error On Gateway	
Agent to Command Engine (CE)	502
Agent to Data Access Engine (DAE)	508
Agent to Software Repository (SWR)	513
NAS Duplex Data Gathering diagnostic	353, 371
NAS Topology Data Gathering diagnostic	353
NAT tables	
changing, affects of	279
See also static NAT.	
navigating	
Opware SAS Web Client	64
SAS Client	75
navigation panel, overview	67
network	
configuring for servers	
overview	346
network interfaces	355
network ports	355
network reports	372
network scripts	559, 560, 562
no callback from Agent, Agent to Command Engine (CE)	504
No Gateway Defined	
Agent to Command Engine (CE)	502
Agent to Data Access Engine (DAE)	507
Agent to Software Repository (SWR)	513
nodes	
configuration tracking policies for	464
entries for configuration tracking, overview	469
notifying, jobs	331

O

ODAD. See Opware Discovery and Agent Deployment.	
OGFS	565
OK	
Agent to Command Engine (CE)	499

- Agent to Data Access Engine (DAE) 505
- Agent to Software Repository (SWR) 510
- Command Engine to Agent (AGT) 493
- Crypto Match (CRP) 497
- Machine ID Match (MID) 515
- Old Agent Version
 - Agent to Command Engine (CE) 501
 - Agent to Data Access Engine (DAE) 506
 - Agent to Software Repository (SWR) 511
- opening
 - remote terminal 144
 - remote terminal session, unmanaged server . . 122
 - remote terminal, managed server to 398
- operating systems
 - provisioning, overview 42
- Opsware administrator, definition of 590
- Opsware Agent
 - Agent upgrade tool 538
 - Communication Test 125
 - definition of 590
 - dormant, definition of 587
 - installation and functionality, verifying 533
 - Installer 523
 - Installer options 528
 - installing 527
 - installing, using ODAD 116
 - limits of functionality on servers 102
 - overview 52, 99
 - running, in a dormant mode 522
 - server data tracked by 103
 - Uninstaller options 535
 - uninstalling 535
- Opsware Agent Installer
 - command line options 528
 - commands and options, examples 532
 - definition of 583
 - uninstaller options 535
- Opsware Agent Uninstaller, definition of 583
- Opsware Discovery and Agent Deployment
 - creating reports 123
 - definition of 591
 - installing, Opsware Agents 116
 - opening remote terminal sessions, unmanaged
 - server to 122
 - overview 45
 - permissions required 115
 - requirements 115
 - specifying
 - deployment actions 109
 - login settings 110
 - viewing
 - history, unmanaged server of 121
- Opsware Gateway, definition of 591
- Opsware Global File System
 - accessing with ssh 386
 - copying files to 389
 - definition of 591
- Opsware guides
 - contents of 29
 - conventions used 31
 - documentation set 33
 - icons in guide, explained 32
- Opsware model space 377
- Opsware model space, definition of 591
- Opsware SAS
 - agent-server architecture 52
 - Code Deployment & Rollback, features 439
 - core, definition of 591
 - documentation set 33
 - features, definition of 590
 - installation, definition of 591
 - model-based approach, affecting servers 53
 - related documentation 33
 - supported operating systems 232, 234
 - types of users 37
- Opsware SAS Web Client
 - accessing 60
 - administration features 67
 - Code Deployment, in navigation 66
 - Environment, in navigation 65
 - Home page, overview 65
 - icon tooltips 69
 - icons for servers, defined 207, 311
 - My Customers, overview 63
 - My Jobs
 - in navigation 65
 - overview 62
 - My Servers, overview 68
 - navigating, overview 67
 - navigation panel, overview 64
 - Reports, in navigation 67
 - server lists, filtering 238
 - Servers, in navigation 65
 - Software, in navigation 65
 - tasks, overview 62
 - ways to search 243
- Opsware Satellite, definition of 591
- options
 - SAS Client, accessing 87
 - unmanaged servers, SAS Client 88
- OS Build Agents
 - definition of 591

OS media, definition of591

OS provisioning

- definition of591
- import media tool, definition of588
- media resource locators (MRLs), definition of589
- media server, definition of589

OS Build Agents

- definition of591
- overview 42

P

packages

- definition of592
- deprecated, definition of586
- viewing

 - installed packages151

packaging server

- definition of592

passwords, selecting 59

patch management

- definition of592
- patch administrators

 - definition of592

performing

- manual backups of tracked configurations477
- sequences for CDR457
- services by hostname for CDR455
- services by service name for CDR453
- services, synchronizations, and sequences,

 - overview443
 - synchronizations for CDR445

permissions

- ODAD, required for115
- server groups, required for281
- setting

 - Global Shell permissions553

port open on managed server, verifying517

post-install script, definition of592

post-uninstall script, definition of592

preferences

- general options, SAS Client 87
- packaging servers, SAS Client91
- terminal and shell, SAS Client92

pre-install script, definition of592

preparing, installing Opware Agents, for523

pre-uninstall script, definition of592

preview remediate

- definition of592

primary IP, definition of276, 593

private device groups164

private group, definition of 593

private, server groups 283

properties

- editing for servers320
- servers, overview316

public device group163

public group, definition of 593

public, server groups283

push561

PuTTY92

Q

QNumber 153, 154, 182

R

RDP 92

reach561

Realm is Unreachable

- Agent to Command Engine (CE)501
- Agent to Data Access Engine (DAE)507
- Agent to Software Repository (SWR)512
- Command Engine to Agent (AGT)495

realm, definition of 593

reconciling, customized tracking policies475

reference server, definition of593

refreshing

- virtual servers197

registry (Windows), browsing, Device Explorer ...156

remediate

- definition of593
- output

 - definition of593

- preview

 - definition of592

remote Opware shell

- definition of594
- modes of operation561
- options and commands559
- overview558

remote terminal

- definition of593
- opening

 - managed server for398
 - overview144
 - unmanaged servers to122

- overview397

removing

- earlier versions of Opware Agents from servers

 - UNIX536

- Windows537
 - Opware Agent, UNIX and Windows535
 - servers
 - from My Servers241
 - from server groups303, 304
 - from service levels344
 - servers from a device group173
 - removing Solaris local zones223
 - renaming files, Device Explorer's File System of .150
 - reports
 - overview267
 - Request Time-out, (AGT)494
 - requirements, running SAS Client for72
 - resolving
 - hostname519
 - script time out events427
 - script uploading errors427
 - restarting, an Opware Agent518
 - restoring
 - backed up files for configuration tracking485
 - code and content from old version for CDR . . .451
 - tracked configurations485
 - rolling back
 - code and content to previous version for CDR 451
 - definition of594
 - restored files for configuration tracking488
 - rosh. See remote Opware shell.
 - rsync389
 - RunCommandOnServer561
 - running
 - Communication Test
 - individual server133
 - multiple servers134
 - custom extensions429
- S**
- SAS Client
 - accessing75
 - general options87
 - installing72
 - options, accessing87
 - overview71
 - packaging servers preferences91
 - requirements72
 - terminal and shell preferences92
 - unmanaged servers options88
 - SAS Web Client
 - My Jobs
 - definition of590
 - SAS Web Client. See Opware SAS Web Client.
 - scan timeout (VAM)95
 - scheduling
 - server jobs330
 - time outs affecting333
 - scp389
 - script management
 - functionality for401
 - tasks, tips, procedures404
 - scripts
 - creating405
 - creation tips405
 - deleting408, 410, 411
 - Distributed Scripts
 - definition of586
 - overview44, 399
 - editing408
 - error resolution427
 - execution
 - functionality402
 - results402
 - results, tasks423
 - tasks, tips, procedures412
 - investigating
 - non-zero return codes428
 - partial executions428
 - server authentication errors428
 - My Scripts, definition of590
 - post-install script, definition of592
 - post-uninstall script, definition of592
 - pre-install script, definition of592
 - pre-uninstall script, definition of592
 - resolving, time outs427
 - resolving, upload errors427
 - Shared Scripts, definition of596
 - uploading405
 - viewing, version histories412
 - ways to initiate403
 - searching
 - details257
 - examples of258
 - for virtual servers225
 - IP addresses258
 - overview, search feature of68
 - Search box242
 - search feature243, 257
 - server search, definition of595
 - unreachable servers137
 - ways to243
 - security
 - Opware Agents, on servers101
 - server management101

selecting, passwords	59	IP range groups, definition of	588
sequences		IP ranges, definition of	588
editor for CDR, definition of	594	model-based approach	53
performing for CDR	457	multiple facilities, in	53
server baselines, definition of	594	notifying, jobs	331
Server Compliance		scheduling, tasks	330
deleting		server life cycle tasks	318
snapshot	594	Server Not Registered, Command Engine to Agent (AGT)	495
selection criteria		Server Pool	
definition of	594	definition of	595
inclusions/exclusions, definition of	588	overview	235
snapshot		server search, using	293
definition of	596	servers	
job, definition of	596	asset tracking, overview	231
template, definition of	596	assigning to service levels	343
source, definition of	597	association with customers	264
target, definition of	597	authentication errors in scripts, investigating	428
Server Explorer		changing value, custom field for	335
definition of	594	changing, use and stage values	320
server groups		cloning	323
adding, servers and server groups to	302	configuration policies for, definition of	595
characteristics	282	configuration tracking policies, customizing	469
creating	288	configuration tracking policy	464
dynamic groups	291	configuration tracking, entries for	469
static groups	288, 290	custom attributes, deleting	339
criteria for search	293	data tracked by Opware Agents	103
definition of	595	deactivating	322
duplicating	305	deactivating, definition of	586
dynamic, definition of	587	definition of	594
modeling, public groups	284	deleting from the Opware SAS	323
overview	280	DHCP, configuring	347
permissions, required	281	domains for Windows servers, changing	348
private, definition of	593	filtering in server lists	238
public, definition of	593	histories, viewing	267
removing, servers and server groups to	303, 304	history, unmanaged server of	121
static, definition of	597	identifying	260
types		installing Opware Agents	
dynamic	284	augmenting	534
private	283	verifying	533
public	283	jobs	
static	283	scheduling	330
using, server search	293	life cycle	
Server ID, definition of	595	definition of	595
server life cycle, Opware SAS	308	Machine ID, definition of	588
server lists		managed, definition of	588
filtering	238	management IP, definition of	589
overview	235	management of	235
server management		media access control address, definition of	589
definition of	595	model-based approach	53
functions	273	My Servers, removing from	241
groups, definition of	587		

- network configuration
 - configuring346
 - overview345
- opening remote terminal sessions, unmanaged
 - server to122
- opening, remote terminal144
- pre-assimilation checklist524
- preparing for installing Opsware Agents523
- primary IP addresses, setting278
- primary IP, definition of593
- properties
 - editing320
 - overview316
- provisioning, definition of595
- reference server, definition of593
- Search box, using242
- search feature, using243
- searching by IP address258
- searching for242
- See also* server groups.
- Server ID, definition of595
- Service Levels, definition of596
- service levels, removing from344
- source, definition of597
- status, definition of595
- swapping disks, examples262
- tracking policies, viewing474
- viewing
 - history159
 - packages151
- virtual, about185
- See also* server management.
- service levels
 - adding individual341
 - assigning servers to343
 - editing342
 - overview340
 - removing, servers from344
 - ways to view for servers342
- Service Levels, definition of596
- services
 - CDR, overview449
 - code deployment, accessing452
 - definition of595
 - editor for CDR, definition of595
 - overview152
 - performer (production) for CDR, definition of ..595
 - performer (staging) for CDR, definition of595
 - performing by hostname for CDR455
 - performing by service name for CDR453
 - requester (production) for CDR, definition of ..595
 - requester (staging) for CDR, definition of595
 - service-instance for CDR, definition of596
- setting
 - Global Shell permissions553
 - primary IP address, server of278
- setup for servers
 - pre-assimilation checklist524
 - preparation for installing Opsware Agents523
- sftp389
- Shared Scripts
 - definition of596
 - executing414
- snapshot
 - definition of596
 - deleting594
 - job, definition of596
 - template, definition of596
- Software596
- Software Policies, browsing, Device Explorer152
- Software Repository Cache, definition of596
- Software Repository Replicator, definition of597
- Software Repository, definition of596
- Solaris
 - local zones
 - creating214
 - choosing zone definition method** 216
 - defining the zone** 217
 - scheduling the job** 218
 - setting email notification** 219
 - starting the job** 219
 - installing an Opsware Agent on212
 - modifying
 - scheduling the job** 222
 - setting email notification** 222
 - starting the job** 222
 - modifying zone definition221
 - starting and stopping213
- Solaris local zones
 - removing223
 - scheduling the job224
 - starting the job225
- specifying
 - deployment actions, ODAD in109
 - login settings, ODAD in110
- ssh386
- stage values, overview for servers320
- standalone core, definition of597
- starting and stopping Solaris local zones213

static device group164
 static group, definition of597
 static NAT
 changing NAT tables, affects of279
 code deployment and rollback, use with278
 static, server groups283
 supported operating systems
 for managed servers232
 for SAS Client234
 supported, browsers57
 synchronizations
 definition of597
 editor for CDR, definition of597
 performer for CDR, definition of597
 performing for CDR445
 requester for CDR, definition of597
 site code and content, overview443

T

target, definition of597
 telnet92
 templates
 local attachment, definition of588
 time outs
 scripts, resolving in427
 server management jobs333
 transcoding394
 troubleshooting
 partial script executions, investigating428
 script non-zero return codes428
 script time out events427
 script uploading errors427
 unreachable servers491
 Tunnel Setup Error
 Agent to Command Engine (CE)502
 Agent to Data Access Engine (DAE)507
 Agent to Software Repository (SWR)513
 Command Engine to Agent (AGT)496
 tunnel, definition of597
 types of, server groups283

U

Unexpected Error
 Agent to Command Engine (CE)500
 Agent to Data Access Engine (DAE)505
 Agent to Software Repository (SWR)510
 Command Engine to Agent (AGT)493
 Machine ID Match (MID)515
 uninstalling

earlier versions of Opware Agents from servers
 UNIX536
 Windows537
 Opware Agent, UNIX and Windows535
 Untested
 Agent to Command Engine (CE)499
 Agent to Data Access Engine (DAE)505
 Agent to Software Repository (SWR)510
 Command Engine to Agent (AGT)493
 Crypto Match (CRP)497
 Machine ID Match (MID)515
 updating, user profile59
 uploading
 code and content to staging for CDR437
 scripts405
 use values, overview for servers320
 user profile, updating59
 user roles, definition of597
 users, definition of597
 users, of Opware37
 using, server search293

V

value set editor
 definition of598
 verifying
 agent is running516
 port is open on managed server517
 viewing
 backup histories for configuration tracking478
 contents, Device Explorer's File System of148
 history
 server268
 server for159
 unmanaged server of121
 job details in the SAS Client329
 job details in the SAS Web Client327
 list of backup events for configuration tracking 479
 managed servers by communication status ..136
 My Jobs, Communication Test139
 packages151
 script execution results
 immediately425
 stored426
 script version history412
 Scripts list408
 server's configuration tracking policies474
 service levels, ways to342
 status of previous CDR operations460
 virtual servers

in reports	200
in the all managed servers list	196
in the Device Explorer - Solaris 10	200
in the Device Explorer - VMware ESX	198
in the Visual Application Manager (VAM)	204
virtual relationships	194
Virtualization Director	
creating device groups for	228
key concepts	187
overview	185
permissions overview	187
scan time out preference	95
searching for virtual servers	225
usage examples	187
viewing virtual servers	
in reports	202
in the all managed servers list	196
in the Device Explorer - Solaris 10	200
in the Device Explorer - VMware ESX	198
in the Visual Application Manager (VAM)	204
virtual relationships	194
virtual server status	206
virtualization settings	94
Visual Application Manager (VAM)	
virtualization settings	94
Visual Packager	
definition of	592
overview	49
VMware ESX	
creating device groups for	228
refreshing VMs	197
searching for	225
viewing	
in reports	202
in Visual Application Manager (VAM)	204
VMs and hypervisors in the Device Explorer	198
VMs in the SAS Client	194
virtual server status	206

W

Web services APIs, definition of	598
Web Services Data Access Engine, definition of	598
Windows servers	
changing, domains	348
wizards	
Distributed Script Execution	399
Run Custom Extension	429
working with	
Device Explorer's File System	148

