



Opsware[®] SAS 6.0 Planning and Installation Guide

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 5.5.1

Copyright © 2000-2006 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Opware Inc. Unpublished Confidential Information.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, Opware Command Center, 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/sas600tpos.pdf>.

Table of Contents

| | |
|---|-----------|
| Preface | 11 |
| <hr/> | |
| Overview of this Guide | 11 |
| Contents of this Guide | 11 |
| Conventions in this Guide | 13 |
| Icons in this Guide | 14 |
| Guides in the Documentation Set and Associated Users | 15 |
| Opsware, Inc. Contact Information | 15 |
| | |
| Chapter 1: Opsware SAS Architecture | 17 |
| <hr/> | |
| Overview of Opsware SAS Architecture | 17 |
| Agent-Server Architecture of Opsware Technology | 18 |
| Server Management in Multiple Facilities | 19 |
| Multimaster Support | 21 |
| Opsware SAS Topologies | 22 |
| Benefits of Multimaster Mesh | 22 |
| Example: Multimaster Topologies | 22 |
| Benefits of Opsware Satellites | 24 |
| Example: Satellite Topologies | 24 |
| Opsware SAS Components | 29 |

| | |
|---|-----|
| Boot Server | .32 |
| Build Manager | .32 |
| Command Engine | .32 |
| Data Access Engine | .32 |
| Media Server | .32 |
| Model Repository | .33 |
| Model Repository Multimaster Component | .33 |
| Opware Agents | .33 |
| Dormant Opware Agents | .34 |
| Opware Command Center | .34 |
| OS Build Agent | .35 |
| Software Repository | .35 |
| Software Repository Replicator | .35 |
| Software Repository Cache | .36 |
| Software Repository Multimaster Component | .36 |
| Web Services Data Access Engine | .36 |
| Opware Gateway | .36 |
| Global File System Server | .37 |

Chapter 2: Supported Operating Systems and Hardware Requirements **39**

| | |
|--|------------|
| Supported Operating Systems | .39 |
| Supported Operating Systems for Opware Core Servers | .39 |
| Support Operating Systems for Opware Agents, the Opware Command Center, and the OCC Client | .40 |
| Hardware Requirements for Opware Core Servers | .42 |

| | |
|--|------------|
| CPU Requirements | .42 |
| Memory Requirements | .43 |
| Disk Space Requirements | .43 |
| Opware Core Scalability for Performance | .43 |
| Factors Affecting Performance for an Opware SAS Core | .45 |
| Scaling Opware SAS with Multimaster Mesh | .46 |
| Factors Affecting Performance for an Opware Satellite | .46 |
| Additional Instances of Opware Components and Load Balancing | .47 |
| Chapter 3: Pre-Installation Requirements | 49 |
| Operating System Requirements | .49 |
| Solaris Requirements | .49 |
| Linux Requirements | .51 |
| Network Requirements | .53 |
| Network Requirements within a Facility | .53 |
| Open Ports | .53 |
| Host and Service Name Resolution Requirements | .55 |
| DHCP Proxying | .56 |
| DMZ Network | .57 |
| Patch Management Requirements | .57 |
| Configuration Tracking Requirements | .60 |
| Opware Global File System (OGFS) Requirements | .60 |
| OGFS Store and Audit Hosts | .60 |
| Name Service Caching Daemon (nscd) and OGFS | .61 |
| Time and Locale Requirements | .61 |

| | |
|---|-----------|
| Core Time Requirements | 61 |
| Locale Requirements. | 62 |
| Chapter 4: Installation Overview and Checklists | 63 |
| Types of Opsware SAS Installations | 63 |
| Opsware Core Installation Process Flow | 64 |
| Checklists | 66 |
| Overall Planning Checklist | 67 |
| Specific Core Planning Checklist | 68 |
| Specific Core Requirements Checklist. | 70 |
| Pre-Installation Tasks Checklist. | 72 |
| Post-Installation Tasks Checklist. | 73 |
| Chapter 5: Prerequisite Information for the Installer Interview | 75 |
| Required Information for Running the Installer Interview | 75 |
| Model Repository Prompts | 76 |
| Database (Model Repository) Password Prompts | 79 |
| Opsware Component Password Prompts | 83 |
| Facility Prompts | 85 |
| Opsware SAS Feature Prompts. | 88 |
| Opsware Gateway Prompts | 93 |
| Opsware Global File System Prompts | 94 |
| Uninstallation Prompts. | 96 |
| Opsware Installer | 96 |

| | |
|--|----|
| Installation Media for the Opsware Installer | 97 |
| Opsware Installer Command Line Syntax | 97 |
| Installer Interview | 99 |
| Opsware Installer Logs | 99 |

Chapter 6: Opsware Standalone Installation **101**

| | |
|---|------------|
| Overview of the Standalone Installation | 101 |
| Prerequisites for Installing a Standalone Core | 102 |
| Installing a Standalone Core | 102 |
| Opsware Command Center Web Client | 107 |
| Logging into the Opsware Command Center | 108 |

Chapter 7: Post-Installation Tasks **111**

| | |
|---|------------|
| Setup for Opsware Discovery and Deployment. | 111 |
| Enabling the ODAD Feature for Unix Servers..... | 111 |
| Enabling the ODAD Feature for Windows Servers..... | 111 |
| Installing the Windows Agent Deployment Helper..... | 112 |
| Setting Up NAS Integration | 114 |
| Configuration for the NAS Integration Feature..... | 114 |
| User Permissions for the NAS Integration Feature | 116 |
| DHCP Configuration for OS Provisioning | 117 |

| | |
|--|------------|
| DHCP Software included with the Opware Boot Server..... | 117 |
| Configuring the Opware DHCP Server for OS Provisioning..... | 120 |
| Starting and Stopping the Opware DHCP Server | 122 |
| Configuring an Existing ISC DHCP Server for OS Provisioning..... | 122 |
| Configuring the MS Windows DHCP Server for OS Provisioning | 126 |
| Configuring the Opware and MS Windows DHCP Servers for OS Provisioning | 127 |
| Additional Network Requirements for OS Provisioning | 129 |
| Patch Management on Windows NT 4.0 and Windows 2000 | 130 |
| Creating a Silent Installable Version of IE 6.0 or Later | 130 |
| Adding Instances of the Opware Global File System Server (OGFS) to a Core | 131 |
| | |
| Chapter 8: Opware Multimaster Installation | 133 |
| | |
| Multimaster Installation | 133 |
| Components of Multimaster Installations | 134 |
| Pre-Existing Core Installations..... | 135 |
| Opware Command Center | 135 |
| TIBCO Rendezvous | 135 |
| Prerequisites for a Multimaster Installation..... | 135 |
| Converting a Core from Standalone to Multimaster | 136 |
| Adding a Core to a Multimaster Mesh | 139 |
| Multimaster Post-Installation Tasks | 149 |

| | |
|---|-----|
| Associating Customers with a New Facility | 149 |
| Updating Permissions for New Facilities | 149 |
| Verifying Multimaster Transaction Traffic | 149 |

Chapter 9: Opware Satellite Installation **151**

| | |
|--|------------|
| Overview of Satellite Installation | 151 |
| Satellite Requirements | 152 |
| Open Ports Required for a Satellite | 152 |
| Entries Required in /etc/hosts for a Satellite | 152 |
| Required Packages for SuSE Linux Enterprise Server 9 | 152 |
| Other Requirements for a Satellite | 153 |
| Gateway Configuration for a Satellite | 154 |
| Satellite with a Standalone Core | 154 |
| Satellite in a Multimaster Mesh | 157 |
| Multiple Gateways in a Satellite | 159 |
| Cascading Satellites | 161 |
| Satellite Installation | 162 |
| Required Information for Installing a Satellite | 162 |
| Installing a Satellite | 163 |
| Post-Installation Tasks for a Satellite | 170 |
| Facility Permission Settings | 171 |
| Checking the Satellite Gateway | 171 |
| Enabling the Display of Realm Information | 171 |
| DHCP Configuration for OS Provisioning | 172 |

Chapter 10: What's Next **173**

| | |
|---|------------|
| Configuration for Opware SAS | 173 |
|---|------------|

| | |
|---|------------|
| Chapter 11: Opsware SAS Uninstallation | 175 |
| Overview of Uninstalling Opsware SAS | 175 |
| Procedures for Uninstalling Cores | 176 |
| Uninstalling a Standalone Core | 176 |
| Uninstalling One Core in a Multimaster Mesh | 177 |
| Uninstalling an Entire Multimaster Mesh of Opsware Cores | 179 |
| Decommissioning a Facility in the Opsware Command Center | 179 |
| | |
| Appendix A: TIBCO Rendezvous Configuration for Multimaster | 181 |
| | |
| TIBCO Rendezvous and Opsware SAS | 181 |
| TIBCO Rendezvous Configuration | 181 |
| Running the TIBCO Rendezvous Web Client | 181 |
| Adding a TIBCO Router | 182 |
| Adding a TIBCO Rendezvous Neighbor | 183 |
| Verifying TIBCO Rendezvous Configuration | 183 |
| | |
| Appendix B: Opsware Gateway Properties File | 185 |
| | |
| Syntax of the Opsware Gateway Properties File | 185 |
| Options for the opswgw Command | 194 |
| | |
| Index | 195 |

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.

Overview of this Guide

This guide describes how to use the Opsware Installer to install the software components that make up an Opsware core. It also describes the administrative tasks required prior to installing an Opsware core.

This guide is intended for Unix system administrators, database administrators, and network administrators.

Contents of this Guide

This guide contains the following chapters:

Chapter 1: Opsware SAS Architecture: Provides an overview of Opsware SAS architecture, which is information you will need before installing an Opsware core or Opsware Satellite, and presents some of the different topologies of Opsware SAS. Use this section as a guide in helping you decide which topology is needed for your Opsware SAS installation.

Chapter 2: Supported Operating Systems and Hardware Requirements: Describes the supported operating systems for an Opsware SAS core, managed servers, and the SAS Client. This chapter also describes the hardware requirements for the servers running an Opsware SAS core and provides guidelines on how to distribute Opsware SAS components across the servers running an Opsware SAS core.

Chapter 3: Pre-installation Requirements: Describes the system and network administration tasks that must be performed before you can run the Opsware Installer.

Chapter 4: Installation Overview and Checklists: Describes the types of Opsware SAS installation, the Opsware SAS core installation process, and provides checklists to aid you in gathering required information prior to installing an Opsware SAS core.

Chapter 5: Prerequisite Information for the Installer Interviewer: Lists the information you will be prompted for by the Opsware SAS Installer interviewer. This chapter also provides information about the installer command line syntax, log files, and how the Opsware Installer is distributed on DVDs.

Chapter 6: Opsware Standalone Installation: Describes how to run the Opsware Installer to create a standalone core.

Chapter 7: Post-Installation Tasks: Describes system administration tasks that you must perform after installing a core.

Chapter 8: Opsware Multimaster Installation: Describes how to run the Opsware Installer to upgrade a standalone core to multimaster and install target facilities.

Chapter 9: Opsware Satellite Installation: Describes how to run the Opsware Installer for creating an Opsware satellite realm.

Chapter 10: What's Next: Provides an overview of the configuration tasks required for the Opsware SAS after the core has been installed.

Chapter 11: Opsware Core Uninstallation: Shows how to un-install a standalone core, remove a core from a multimaster mesh, and un-install an entire Opsware SAS made up of multiple cores in different facilities.

Appendix A: TIBCO Rendezvous Configuration for Multimaster: Provides reference information about the TIBCO configuration for multimaster. By default, the Opsware SAS Installer configures TIBCO for a multimaster mesh.

Appendix B: Opsware Gateway Properties File: Provides reference information about the settings in the properties file used by the Opsware Gateway.





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, Opsware 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 iconographic conventions.

| 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 *Opsware® SAS User's Guide: Server Automation* is intended to be read by systems administrators and 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, remediating servers, script execution, configuration tracking, deploying and rolling back code, agent deployment, and using the Opsware Global Shell and opening a Remote Terminal on managed servers. This guide is intended for system administrators who are responsible for all aspects of managing the servers in an operational environment.
- *Opsware® SAS User's Guide: Server Automation* is intended to be read by the system administrator who is responsible for performing the day-to-day functions of managing servers, such as auditing and compliance, software packaging, visual application management, application configuration, and installing software and operating systems on managed servers.
- The *Opsware® SAS Administration Guide* is intended to be read by Opsware administrators who will be responsible for monitoring and diagnosing the health of the Opsware SAS components.
- The *Opsware® SAS Planning and Installation Guide* is intended to be used by advanced system administrators who are responsible for planning all facets of an Opsware SAS installation and for the installation of Opsware SAS in a facility. It documents all the main features of Opsware SAS, scopes out the planning tasks necessary to successfully install Opsware SAS, how to run the Opsware Installer, and how to configure each of the components. It also includes information on system sizing and checklists for installation.
- The *Opsware® SAS Policy Setter's Guide* is intended to be used by system administrators who are responsible for all facets of configuring the Opsware Command Center. It documents how to set up users and groups, how to configure Opsware server management, and how to set up the main Opsware Command Center features, such as patch management, configuration tracking, software repository replicator setup, code deployment, and software provisioning.

Opsware, Inc. Contact Information

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

- <http://www.opsware.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.opsware.com/opsw/main.htm>

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

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

The Opware Customer Support email address and phone number follow:

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

Chapter 1: Opware SAS Architecture

IN THIS CHAPTER

This section discusses the following topics:

- Overview of Opware SAS Architecture
- Opware SAS Topologies
- Opware SAS Components

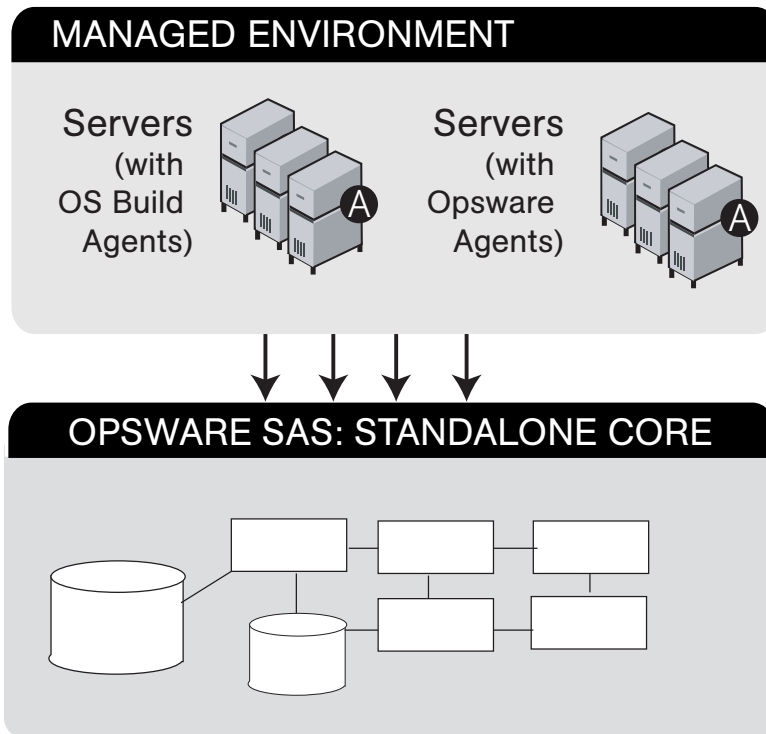
Overview of Opware SAS Architecture

This chapter provides an overview of Opware SAS architecture, which is information you will need before installing an Opware core or Opware Satellite. Second, this chapter presents some of the different topologies of Opware SAS. Use this chapter as a guide in helping you decide which topology is needed for your Opware SAS installation.

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 1-1: Opware SAS Agent-Server 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 Opware 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.

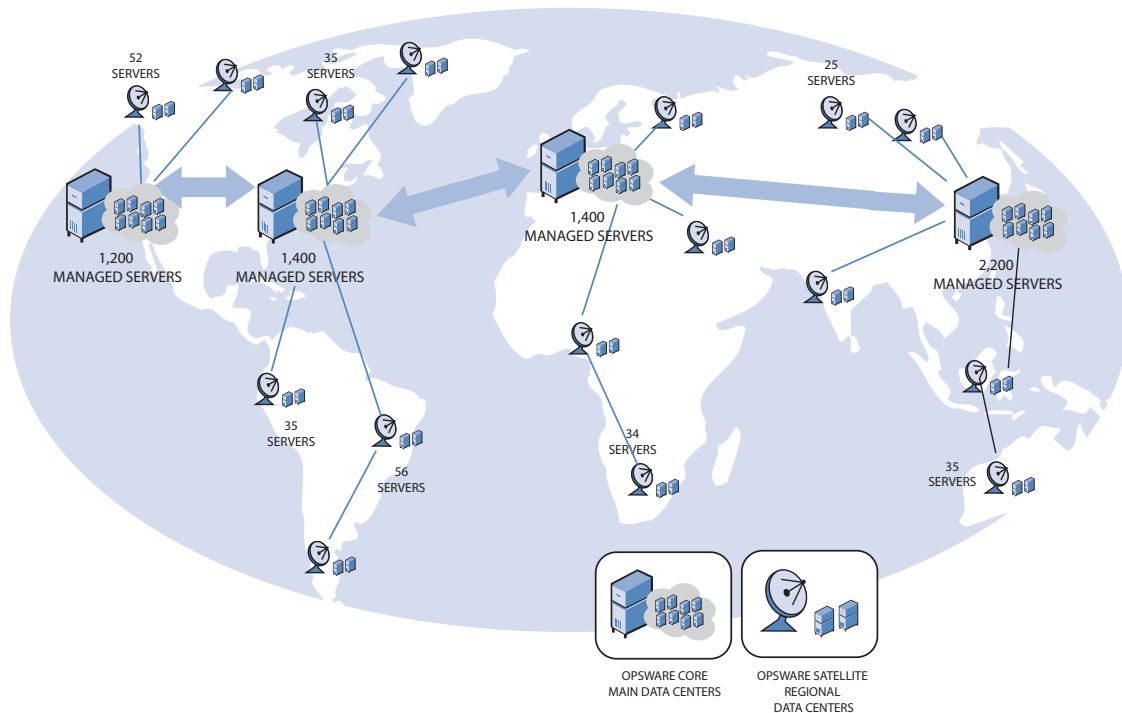
After you install an Opsware Agent on a server, users can manage the server by installing or upgrading software, patching the OS software, removing software, changing server properties, or decommissioning the server.

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.

Figure 1-2: Server Management in Multiple Facilities



Users can manage servers in any facility from an Opware Command Center or a SAS 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:

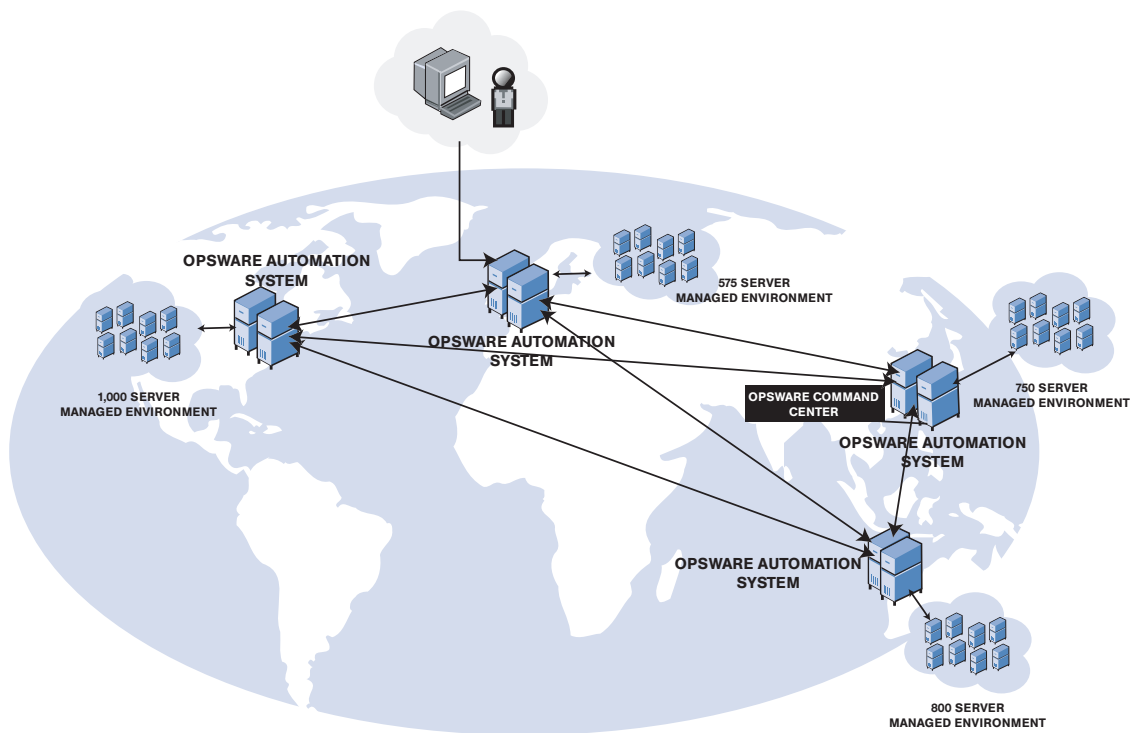
- Users should not change data in one facility and then make the same change in another facility.
- More than one user should not change the same object in different facilities at the same time. For example, two users should not manage the same server from different facilities.

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 Command Center) 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.

Figure 1-3: Multimaster Support



Opsware SAS Topologies

Opsware SAS requires at least one Opsware core. The simplest topology is a single, standalone core that manages servers in a single facility. To manage servers in more than one facility, you should install either a multimaster mesh of cores, Opsware Satellites, or a combination of both. For more information, see the *Opsware® SAS Deployment and Installation Guide* and the *Opsware® SAS Administration Guide*.

Benefits of Multimaster Mesh

To manage servers in large, geographically dispersed facilities, you should consider installing a core in each facility, linked in a multimaster mesh. In a multimaster mesh of cores, data is updated locally and then propagated to every Opsware Model Repository (database) in the mesh. A multimaster mesh offers the following benefits:

- **Redundancy:** Management of data is synchronized between facilities in a multimaster mesh. If the Opsware core in one facility is damaged, another core in the multimaster mesh contains a synchronized copy of the data. Also, it provides the ability to move out of a facility and keep Opsware SAS running in other facilities.
- **Performance Scalability:** An Opsware core can operate on servers in the local facility independently of the processing in the other facilities in the mesh. Only the load of the multimaster database synchronizations are transmitted between facilities.

Write operations do not need to be proxied to a central location.

- **Geographic Scaling:** International facilities can be independent and do not need to rely on a network connection across continents to a central facility.

Example: Multimaster Topologies

Figure 1-4 shows an multimaster mesh with a core in two facilities. Each core contains a Model Repository with data that is synchronized with the other repository. This synchronization data passes through the core Gateways. The managed servers (indicated in the figure with the letter "A") communicate with the core via the Agent and core Gateways. If one core becomes unavailable, the managed servers in that core can still be operated on with the Opsware Command Center of the other core.

See “Model Repository” on page 33 and “Opsware Gateway” on page 36 for a description of these Opsware SAS components.

Figure 1-4: Multimaster Mesh With Two Cores

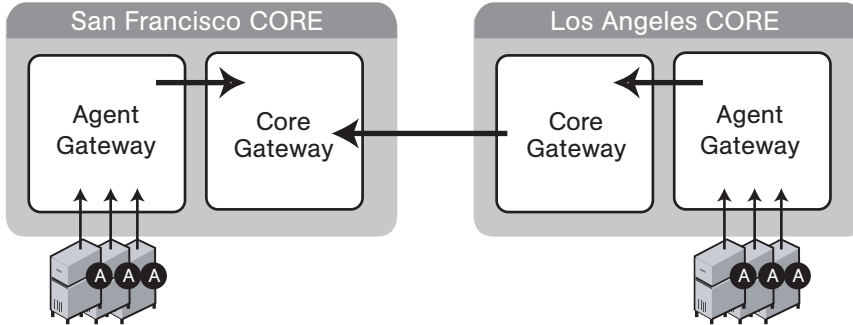
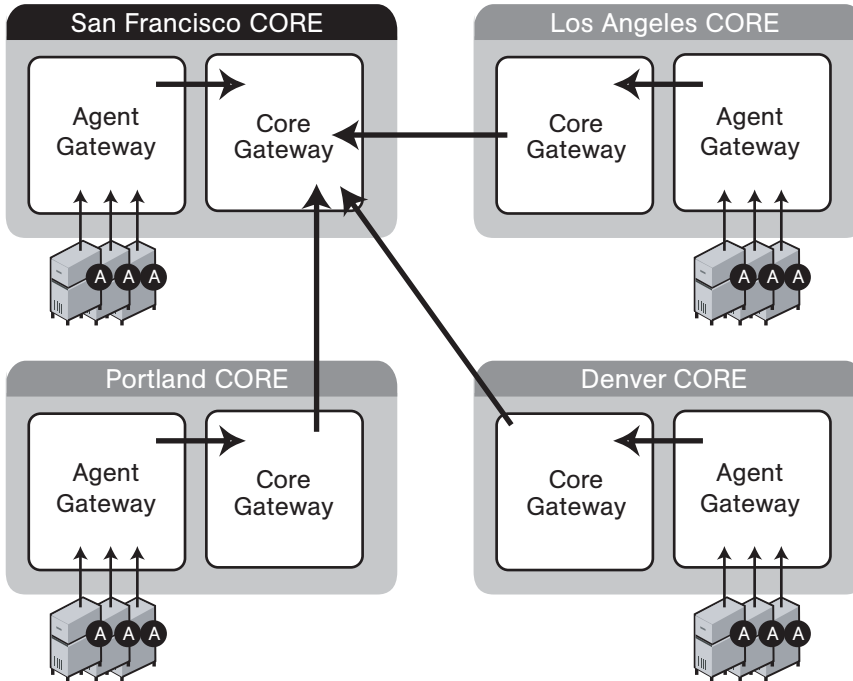


Figure 1-5 shows a multimaster mesh with several cores. This topology is in a star format with the San Francisco core at the center of the mesh. By default, the Opsware Installer configures a multimaster mesh with a star topology.

Figure 1-5: Multimaster Mesh With Four Cores



Benefits of Opsware Satellites

To manage servers in a small, remote facility, you should consider installing a Satellite in the remote facility instead of another core. Opsware Satellites offer the following benefits:

Management of servers with overlapping IP addresses: Servers in different facilities might have overlapping IP addresses. This situation can occur when servers in remote facilities are behind NAT devices or firewalls. The Opsware realm name plus the IP address uniquely identifies a managed server. A realm is a logical name for a group of IP addresses that can be contacted by a particular set of Gateways. Servers with overlapping IP addresses must reside in separate Opsware realms.

Network bandwidth management: Opsware SAS might share the network connection between the Satellite and the core with other applications. If this network connection has limited bandwidth, you might want to limit the network bandwidth used by Opsware SAS. You can limit the bandwidth by configuring the Opsware Gateway in the Satellite. The Opsware Gateway can manage bandwidth on a tunnel-by-tunnel basis.

Example: Satellite Topologies

Figure 1-6 shows a single Opsware Satellite linked to a standalone core. In this example, the main facility is in San Francisco, and a smaller remote facility is in San Jose. The core is made up of several components, including the Software Repository, the Model Repository, and two gateways. The figure does not show other required core components, such as the Command Engine, but indicates them with an ellipsis (...) button. When you install a standalone core, the Opsware Installer creates both the Agent and core Gateways. A Satellite can contain a Software Repository Cache, a Gateway, an OS Provisioning Boot Server, and an OS Media Boot Server.

See “Software Repository Cache” on page 36, “Boot Server” on page 32, and “Media Server” on page 32 for a description of these Opsware SAS components.

The Software Repository Cache contains local copies of software packages to be installed on managed servers in the Satellite. The Agents in the San Francisco facility communicate with the core through the Agent Gateway. The Agents in the San Jose facility connect to the San Francisco core via the Satellite Gateway.

Figure 1-6: Satellite With Standalone Core

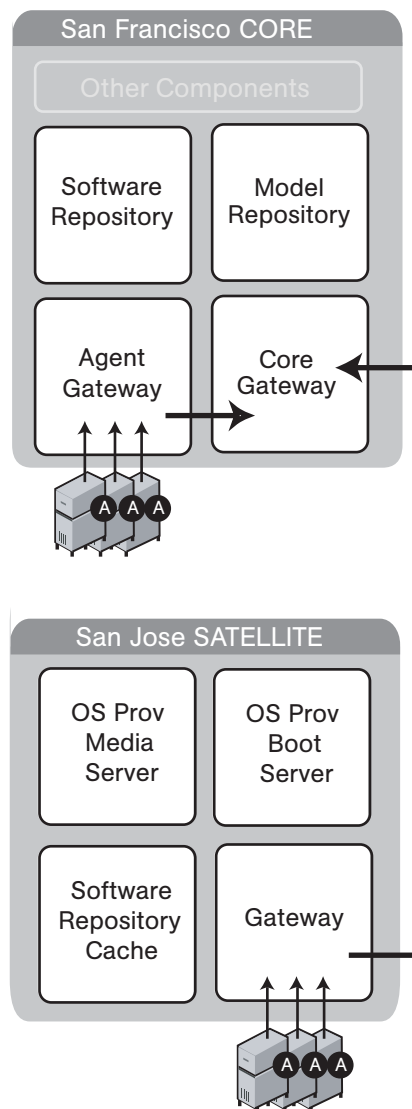


Figure 1-7 shows two Satellites linked to a standalone core. In this example, San Francisco, Sunnyvale, and San Jose are separate facilities. San Francisco is the large primary facility. Sunnyvale and San Jose are small remote facilities.

Figure 1-7: Two Satellites With a Standalone Core

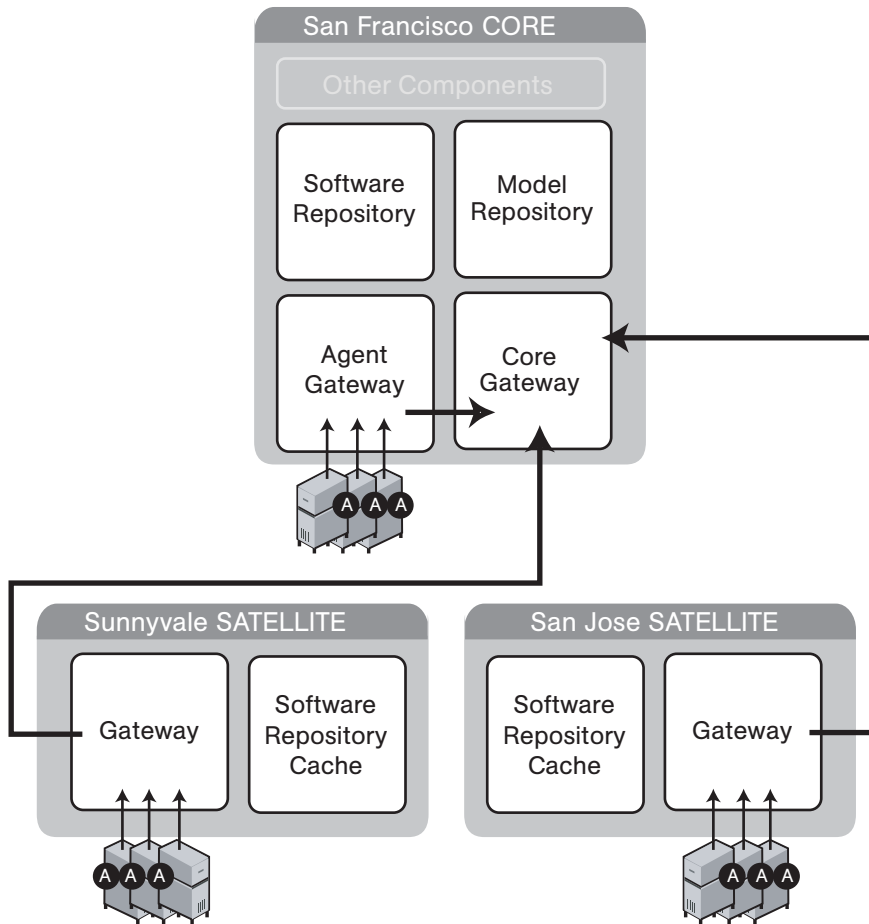


Figure 1-8 shows cascading Satellites, a topology in which Satellite Gateways are connected in a chain. This topology enables you to create a hierarchy of Software Repository Caches. The Satellite Gateways in this topology must belong to different realms. To install a package on a managed server in the Sunnyvale facility, Opware SAS first checks to see if the package resides in the Software Repository Cache in Sunnyvale. If the package is not in Sunnyvale, then Opware SAS checks the Software Repository

Cache in San Jose. Finally, if the package is not in San Jose, Opware SAS goes to the Software Repository in the San Francisco core. For more information, see “Managing the Software Repository Cache” in *Opware[®] SAS Administration Guide*.

Figure 1-8: Cascading Satellites With a Standalone Core

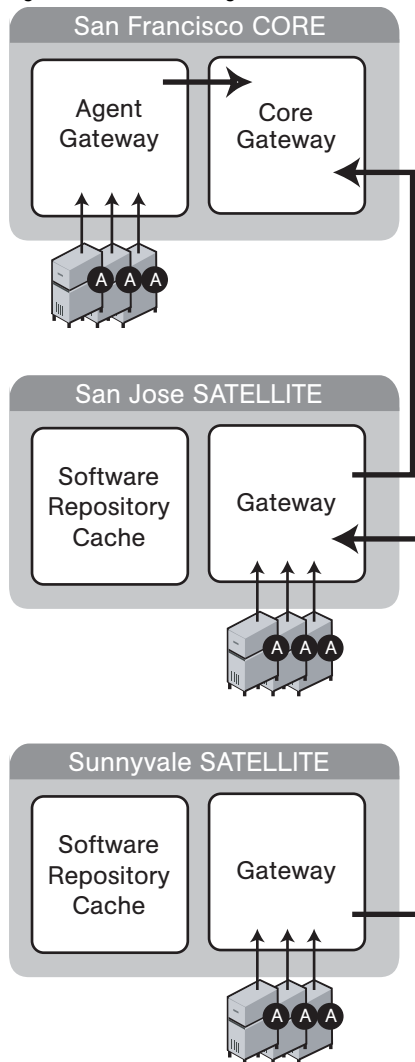


Figure 1-9 shows a Satellite connected to two cores in a multimaster mesh. A Satellite Gateway routes traffic to only one core Gateway at any given time. The Gateway chooses the route with the lowest cost, a parameter specified during Gateway installation. Suppose that the cost of the link between the San Jose and San Francisco is the lowest.

During normal operations, the servers in San Jose are managed by the San Francisco core. If the connection between San Jose and San Francisco fails, then the Gateway in San Jose will communicate instead with the core in Los Angeles.

Figure 1-9: Satellite in a Multimaster Mesh

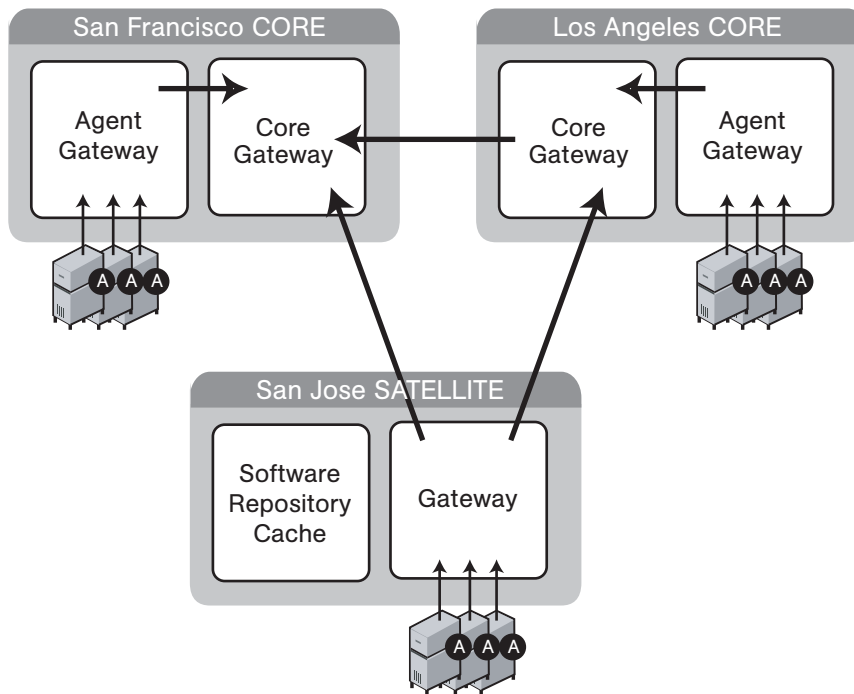
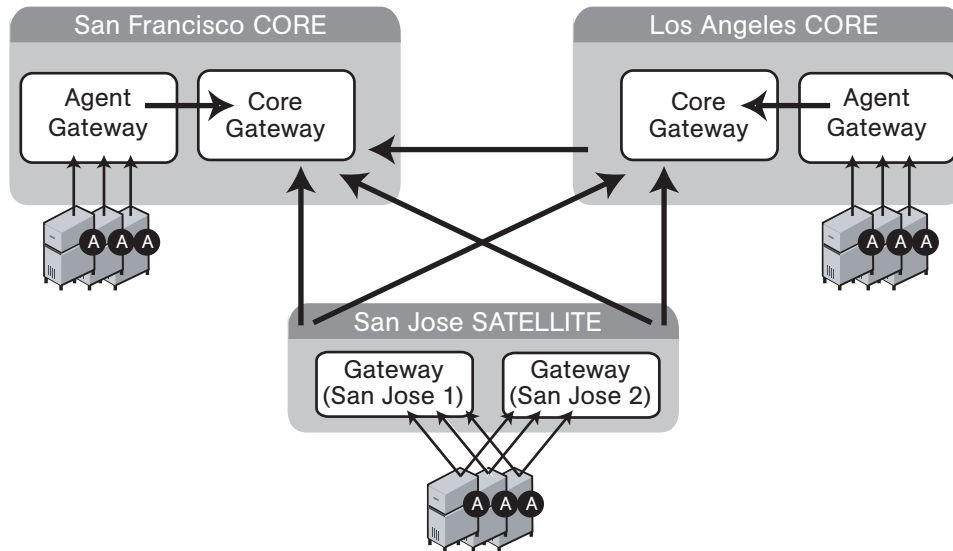


Figure 1-10 shows a topology that provides failover capability in two ways. First, the Gateway in each Satellite has connections to both core Gateways. If one core becomes unavailable, the other core can manage the servers in the Satellite. Second, the Agents in the Satellite point to both Satellite gateways. Opsware Agents automatically load balance themselves over the available gateways in a Satellite.

If one Gateway becomes unavailable, the Agents that are using the unavailable gateway as their primary gateway will automatically failover to using the secondary gateway. During routine agent-to-core communication, Opware Agents will over time discover new gateways added to (or removed from) a multimaster mesh.

Figure 1-10: Satellite With Multiple Gateways in a Multimaster Mesh



Opware SAS Components

Opware SAS has an agent-server architecture. Each server managed by Opware SAS runs an Opware Agent, which performs tasks remotely. The server portion of Opware SAS is called the Opware core, consisting of multiple, integrated components, each with a unique purpose.

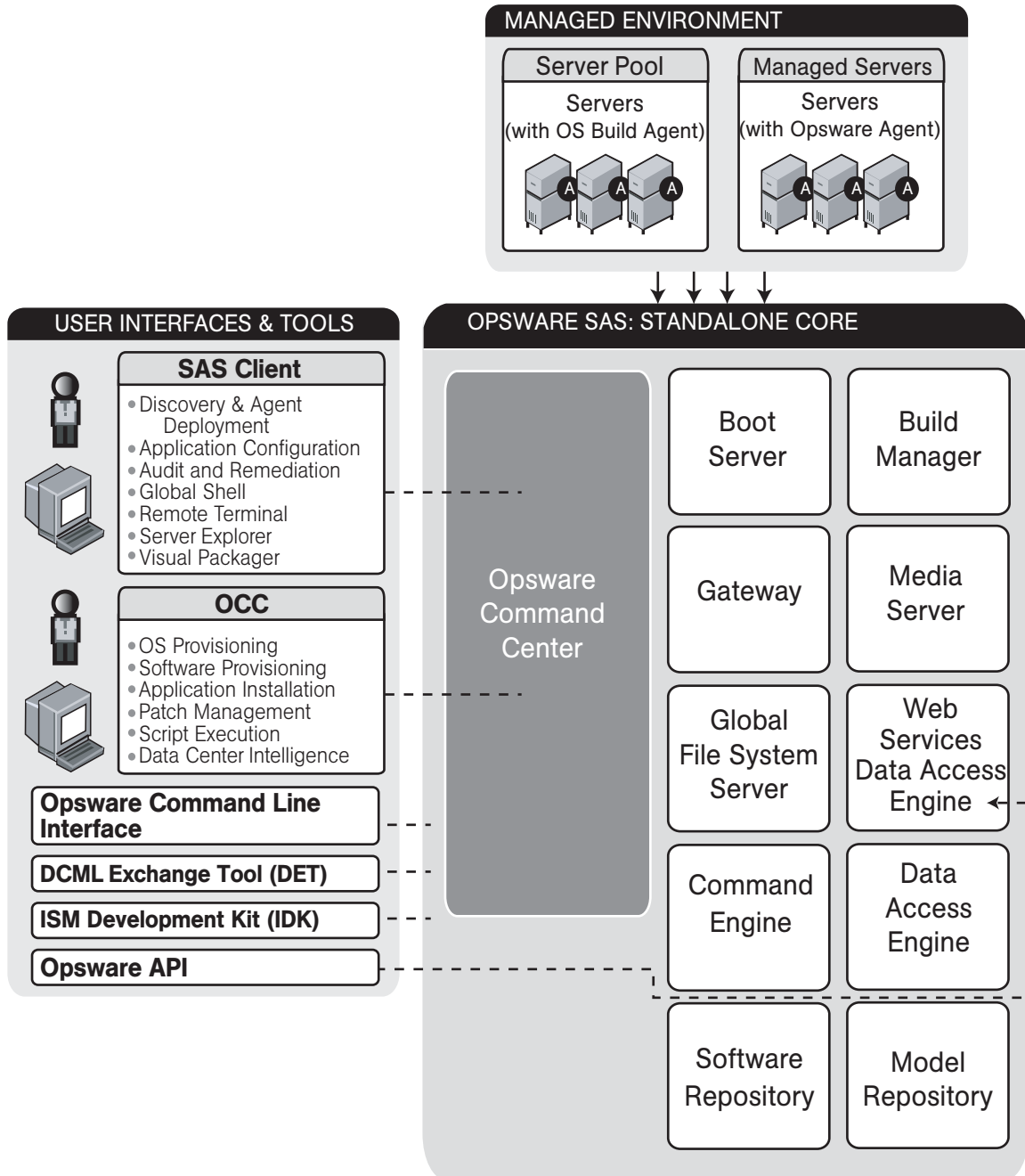
The sections that follow describe the components of Opware SAS:

- **Boot Server:** Part of the OS Provisioning feature that supports network booting of Sun and x86 systems.
- **Build Manager:** This facilitates communication between components for OS provisioning.
- **Command Engine:** The system for running distributed programs across many servers.
- **Data Access Engine:** The XML-RPC interface to the Model Repository.
- **Media Server:** This server provides network access to vendor-supplied media used during OS provisioning.

- **Model Repository:** The Opware SAS data repository (database).
- **Model Repository Multimaster Component:** The application that propagates and synchronizes changes from each Model Repository database to all other Model Repository databases.
- **Opware Agents:** Intelligent agents that run on each server that Opware SAS manages.
- **Opware Command Center:** The user interface to Opware SAS.
- **OS Build Agent:** The agent responsible for registering a bare metal server with Opware SAS and guiding the OS installation process.
- **Software Repository:** The central repository for all software that Opware SAS manages.
- **Software Repository Replicator:** This serves as backup for Software Repositories in a multimaster mesh, ensuring that packages are available, even if one of the Software Repositories becomes unavailable.
- **Software Repository Multimaster Component:** This aids in transferring software from the Software Repository in one facility to the Software Repository in another facility in a multimaster mesh.
- **Software Repository Cache:** This contains local copies in the Opware Satellite of the Software Repository of the core (or another Satellite).
- **Web Services Data Access Engine:** This provides increased performance from the Model Repository to other Opware SAS components.
- **Opware Gateway:** This provides network connectivity to Opware cores and Satellites.
- **Global File System Server:** This dynamically constructs the Opware Global File System (OGFS), a virtual file system.

The following figure shows an overview of Opware SAS components in a standalone core. The components in a core can be distributed across multiple servers.

Figure 1-11: Overview of the Opware Components



Boot Server

The Boot Server, part of the OS Provisioning feature, 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

The Build Manager component facilitates communications between OS Build Agents and the Command Engine. It accepts OS provisioning commands from the Command Engine, and it provides a runtime environment for the platform-specific build scripts to perform the OS provisioning procedures.

Command Engine

The Command Engine is a system for running distributed programs across many servers (usually Opware Agents). Command Engine scripts are written in Python and run on the Command Engine server. Command Engine scripts can issue commands to Opware Agents. These calls are delivered in a secure manner and are auditable by using data stored in the Model Repository.

Opware SAS features (such as Code Deployment & Rollback) can use Command Engine scripts to implement part of their functionality.

Data Access Engine

The Data Access Engine provides an XML-RPC interface to the Model Repository that simplifies interaction with various clients such as the Opware Command Center, system data collection, and monitoring agents on servers.

Because interactions with the Model Repository go through the Data Access Engine, clients are less impacted by changes to the Model Repository's schema. The Data Access Engine allows features to be added to Opware SAS without requiring system-wide changes.

Media Server

The Media Server is also part of the OS Provisioning feature, and is responsible for providing network access to the vendor-supplied media used during OS provisioning. The processes used to provide this support include the Samba SMB server and Sun Solaris NFS.

Model Repository

The Model Repository is implemented as an Oracle database. All Opsware SAS components work from, or update, a data model maintained for all servers that Opsware SAS manages. The Model Repository contains essential information necessary to build, operate, and maintain the following items:

- A list of all servers under management.
- The hardware associated with these servers, including memory, CPUs, storage capacity, and so forth.
- The configuration of those servers, including IP addresses.
- The operating system, system software, and applications installed on servers.
- Information on other software available for installation on servers and how it is bundled
- Authentication and security information.

Each Opsware core, whether standalone or multimaster, contains a single Model Repository. An Opsware Satellite, which relies on a core, does not contain a Model Repository.

Model Repository Multimaster Component

The Model Repository Multimaster Component is installed in a core that belongs to a multimaster mesh. The Model Repository Multimaster Component synchronizes the data in the Model Repositories of the mesh, propagating changes from one repository to another. Every Model Repository instance has one Model Repository Multimaster Component instance. The Model Repository Multimaster Component uses TIBCO Rendezvous.

Each Model Repository Multimaster Component consists of a sender and a receiver. The sender (Outbound Model Repository Multimaster Component) polls the Model Repository and sends unpublished transactions. The receiver (Inbound Model Repository Multimaster Component) accepts the transactions and applies them to the local Model Repository.

Opsware Agents

Each server that Opsware SAS manages has an intelligent agent running on that server. The Opsware Agent is the agent of change on a server. Whenever Opsware SAS needs to make changes to servers, it does so by sending requests to the Opsware Agent.

Depending on the request, the Opsware Agent might use global Opsware SAS services (such as the Model Repository and Software Repository) in order to fulfill the request.

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 Model Repository and registers itself, which allows the Model Repository to keep track of machine status, and know when particular servers are disconnected from and reconnected to the network.

Dormant Opsware Agents

The Opsware Agent Installer can install Opsware Agents even when Opsware SAS core is not available to a server. If a newly-installed Opsware Agent cannot contact an Opsware SAS core, the Opsware Agent runs in a dormant mode. While dormant, it periodically attempts to contact Opsware SAS core.

When Opsware SAS core becomes available, the Opsware Agent performs the initialization tasks, such as hardware and software registration, that usually take place when the Opsware Agent is first installed.

Opsware Command Center

The Opsware Command Center is a user interface to Opsware SAS. Through the web-based user interface, an Opsware SAS user can provision and maintain systems, and deploy code and content to servers. An Opsware administrator adds users and defines access to specific Opsware SAS resources.

The Opsware Command Center talks primarily to the Data Access Engines (which communicate with the Model Repository), though they also talk directly to other back-end services to implement some operations. Users accessing the Opsware Command Center are authenticated before they gain access.

OS Build Agent

The OS Build Agent, part of the OS Provisioning feature, is responsible for registering bare metal servers in Opware SAS. In addition, it is the agent of change on the server during the OS installation process (that the Build Manager manages) until the actual Opware Agent is installed.

Software Repository

The Software Repository is the central repository for all software that Opware SAS manages. It contains packages for operating systems, applications (for example, BEA WebLogic or IBM WebSphere), databases, customer code, and software configuration information.

Working with the Software Repository, an Opware Agent can install software running on the server where the Opware Agent is installed. The Model Repository then updates its record of the software installed on the server. This process of updating the actual software configuration of a server with a specified configuration stored in the Model Repository is called reconciliation.

You can install new software, code, or configurations in the Software Repository by first packaging the files, and then uploading them into the Software Repository.

See the *Opware[®] SAS Configuration Guide* for information about how to upload software packages to the Software Repository.

Software Repository Replicator

The Software Repository Replicator provides backup functionality for Software Repositories running in a multimaster mesh. In most deployments, the Software Repositories do not all have the same content. If one of the Software Repositories becomes unavailable, this might result in some packages not being available until the Software Repository is back online.

Using the Software Repository Replicator provides redundant storage of Software Repositories and thereby helps to ensure that all packages remain available even when a Software Repository goes offline.

Software Repository Cache

Installed in an Opware Satellite, a Software Repository Cache contains local copies of the contents of the Software Repository of the core (or of another Satellite). These local copies improve performance and decrease network traffic when the core installs or updates software on the managed servers in the Satellite.

Software Repository Multimaster Component

The Software Repository Multimaster Component allows software to be distributed across several Software Repositories and to be transferred from one repository to another on-demand. For example, a Solaris package that resides on Software Repository (A) is needed for installation in a second facility that contains Software Repository (B), which is part of the same multimaster mesh. The Multimaster Component allows B to discover the presence of the package on A. The package is then transferred and cached at B so that it can be used in the second facility.

Web Services Data Access Engine

The Web Services Data Access Engine provides a public object abstraction layer to the Model Repository. This object abstraction can be accessed through a Simple Object Access Protocol (SOAP) API by third-party integration components, or it can be accessed through a binary protocol by Opware SAS components like the Opware Command Center. It provides increased performance to other Opware SAS components.

Opware Gateway

The Opware Gateway allows an Opware core to manage servers that are behind one or more NAT devices or firewalls. Connectivity between gateways is maintained by routing messages over persistent TCP tunnels between the gateway instances.

Additionally, the gateway provides network bandwidth management between Opware cores in a multimaster mesh and between cores and Satellites. The ability to manage network bandwidth is important when a tunnel between gateway instances transits a low-bandwidth link, which might be shared with a bandwidth-sensitive application.

One or more Opware Gateways 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.

Global File System Server

The Opsware Global Shell feature runs on the Global File System Server, which dynamically constructs a virtual file system – the Opsware Global File System (OGFS). The Global File System Server component is installed on a Linux server in an Opsware core. The Global File System Server can connect to an Opsware Agent to open a Unix shell or a Windows Remote Desktop connection on a managed server.

Chapter 2: Supported Operating Systems and Hardware Requirements

IN THIS CHAPTER

This section discusses the following topics:

- Supported Operating Systems
- Hardware Requirements for Opsware Core Servers
- Opsware Core Scalability for Performance

Supported Operating Systems

This section discusses the following topics:

- Supported Operating Systems for Opsware Core Servers
- Support Operating Systems for Opsware Agents, the Opsware Command Center, and the OCC Client

Supported Operating Systems for Opsware Core Servers

This section lists the supported operating systems for Opsware core components.

The following table lists the supported operating systems for the Opsware core components (other than the Global File System Server). The Global File System server can be installed only on Red Hat Enterprise Linux 3 AS. Therefore, a single-server installation is supported only on Red Hat Enterprise Linux 3 AS.

Table 2-1: Opsware Core Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE CORE | VERSIONS | ARCHITECTURE |
|--|-------------------------------|------------------------|
| Sun Solaris | Solaris 8 Solaris 9 | Sun SPARC Sun SPARC |
| Red Hat Linux | Red Hat Enterprise Linux 3 AS | 32 bit x86 |

For a list of supported Oracle versions for the Model Repository, see Appendix A in the *Opware® SAS Deployment and Installation Guide*.

The following table lists the supported operating systems for the Gateway and Software Repository Cache components of an Opware Satellite..

Table 2-2: Opware Satellite Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE SATELLITE (GATEWAY AND SOFTWARE REPOSITORY CACHE COMPONENTS) | VERSIONS | ARCHITECTURE |
|--|--------------------------------|--------------|
| Sun Solaris | Solaris 9 | Sun SPARC |
| Red Hat Linux | Red Hat Enterprise Linux 3 AS | 32 bit x86 |
| SUSE Linux | SUSE Linux Enterprise Server 9 | 32 bit x86 |

Support Operating Systems for Opware Agents, the Opware Command Center, and the OCC Client

This section lists the supported operating systems for Opware Agents, the Opware Command Center, and the OCC Client.

The following table lists the supported operating systems for Opware Agents, which run on the servers managed by Opware SAS.

Table 2-1: Opware Agent Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT | VERSIONS | ARCHITECTURE |
|---|----------|--------------|
| AIX | AIX 4.3 | POWER |
| | AIX 5.1 | POWER |
| | AIX 5.2 | POWER |
| | AIX 5.3 | POWER |

Table 2-1: Opsware Agent Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT | VERSIONS | ARCHITECTURE |
|---|--|--|
| HP-UX | HP-UX 10.20 HP-UX 11.00 HP-UX 11.11 HP-UX 11i v2 | PA-RISC PA-RISC PA-RISC PA-RISC and Itanium |
| Sun Solaris | Solaris 6 Solaris 7 Solaris 8 Solaris 9 Solaris 10 | Sun SPARC Sun SPARC Sun SPARC Sun SPARC 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 64 bit x86 |
| Red Hat Linux | Red Hat Linux 7.3 Red Hat Linux 8.0 Red Hat Enterprise Linux 2.1 AS Red Hat Enterprise Linux 2.1 ES Red Hat Enterprise Linux 2.1 WS Red Hat Enterprise Linux 3 AS Red Hat Enterprise Linux 3 ES Red Hat Enterprise Linux 3 WS Red Hat Enterprise Linux 4 AS Red Hat Enterprise Linux 4 ES Red Hat Enterprise Linux 4WS | 32 bit x86 32 bit x86 32 bit x86 32 bit x86 32 bit x86 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86 |

Table 2-1: Opware Agent Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT | VERSIONS | ARCHITECTURE |
|---|--------------------------------|---------------------------|
| 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 |

The following table lists the operating systems supported for the OCC Client.

Table 2-2: OCC 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 - 1.4.2-10 JRE must be installed on the system that runs on the OCC Client. To download this version of Java, go to <http://java.sun.com/j2se/1.4.2/download.html>

Hardware Requirements for Opware Core Servers

An Opware core server is a computer running one or more Opware core components. You can install all of the Opware core components on a single server, or you can distribute the components across multiple servers. The sections that follow describe the hardware requirements for Opware core servers.

CPU Requirements

The CPU for core servers has the following requirements:

- Single-server core: 4 CPUs
- Multiple-server core: 2 CPUs per server

See “Opware Core Scalability for Performance” on page 43 in this chapter for more information.

Memory Requirements

The memory for core servers has the following requirements:

- Single-server core: 4 GB RAM
- Multiple-server core: 2 GB RAM per server

Disk Space Requirements

On each core server, the root directory must have at least 72 GB of hard disk space. (Opware components are installed in the directories `/cust` and `/1c`.) This disk space requirement does not include the requirements for the following components:

- **Model Repository (database):** Additional disk space is required for the Oracle Database product and the data files containing the Model Repository. For information on the Oracle Database product, see the *Oracle Database Installation Guide*. For information on the data file and tablespace requirements, see the *Opware® SAS Deployment and Installation Guide*.
- **Software Repository:** The Software Repository contains software packages and other installable files. Typical installations start with approximately 100 to 200 GB. However, more space might be required, depending on the number and size of the packages, as well as the frequency and duration of configuration backups.
- **Media Server:** This component requires sufficient disk space for the OS media it contains.

Install the Opware components on a local disk, not on a NetApp file server. However, for the Software Repository, you can use a variety of storage solutions, including internal storage, Network Attached Storage (NAS), and Storage Area Networks (SANs).

Opware Core Scalability for Performance

You can scale the Opware core components vertically, by adding additional CPUs and memory, or horizontally, by distributing the components on multiple hardware servers. Table 2-3 lists the recommended distribution of Opware components across multiple servers. The components names in the table have the following abbreviations:

- MR - Model Repository

- MR MM - Model Repository Multimaster Component
- OGFS - Opware Global File System
- OCC - Opware Command Center
- DAE - Data Access Engine
- OS PBM - OS Provisioning Build Manager
- CE - Command Engine
- SR - Software Repository
- GW - Gateway

Table 2-3: Distribution of Core Components

| NUMBER OF CORE SERVERS | OPSWARE CORE COMPONENTS | | | | |
|------------------------|---|---------------------------|-----------|--------|--------|
| | Number of CPUs per Core Server | | | | |
| | 4 CPUs | 2 CPUs | 2 CPUs | 2 CPUs | 2 CPUs |
| 1 | MR MR MM OGFS OCC DAE OS PBM CE SR GW | | | | |
| 2 | MR MR MM OGFS OCC GW | DAE OS PBM CE SR | | | |
| 3 | MR MR MM OGFS GW | DAE OS PBM CE | OCC SR | | |

Table 2-3: Distribution of Core Components

| NUMBER OF CORE SERVERS | OPSWARE CORE COMPONENTS | | | | |
|------------------------|-------------------------|---------------|---------------------|------------|------------|
| | 4 | MR MR MM | DAE OS PBM CE | OCC SR | OGFS GW |
| 5 | MR MR MM | DAE OS PBM | SR CE | OGFS GW | OCC |



If you install core components on multiple servers, do not install the Opware Command Center (OCC) and the Data Access Engine (DAE) on the same server.

Factors Affecting Performance for an Opware SAS Core

The hardware requirements for Opware SAS vary based on the following factors:

- The number of servers that Opware SAS is managing.
- The number and complexity of concurrent operations.
- The number of concurrent users accessing the Opware Command Center.
- The number of facilities in which Opware SAS operates.

Table 2-4 lists the approximate number of core servers required for a given number of managed servers and Opware users.

Table 2-4: Required Number of Core Servers

| NUMBER OF MANAGED SERVERS | NUMBER OF OPSWARE USERS | REQUIRED NUMBER OF CORE SERVERS |
|---------------------------|-------------------------|---------------------------------|
| 480 | 20 | 1 |
| 1125 | 45 | 2 |
| 2250 | 90 | 3 |
| 3600 | 140 | 4 |
| 4000 | 150 | 5 |

Scaling Opsware SAS with Multimaster Mesh

To support global scalability, you can install an Opsware core in each major facility, linking the cores in a multimaster mesh. The size of the Opsware core in each facility can be scaled according to local requirements.

To support availability in a multimaster mesh, you can manage the servers in all facilities from a single location with the Opsware Command Center or a SAS Client. Therefore, the number and location of Opsware Command Center instances and SAS Clients is flexible. A common implementation is with two geographically distributed Opsware Command Centers.

In addition to Model Repository replication, a multimaster mesh supports the replication and caching of the packages stored in the Software Repository. Typically, the Opsware core in each facility owns the software that is uploaded to the core's Software Repository. To support availability, multiple copies of the packages can be maintained in remote Software Repositories. See the *Opsware® SAS Administration Guide* for more information.

Factors Affecting Performance for an Opsware Satellite

Install Opsware Satellites on servers that meet the following requirements:

- 2 CPUs per 500 managed servers
- 2 GB RAM per 500 managed servers

Table 2-5 lists the approximate number of Opsware Satellites required for a given number of managed servers.

Table 2-5: Scaling Opsware SAS with Opsware Satellites

| MANAGED SERVERS | SATELLITES | 10% REDUNDANCY | 20% REDUNDANCY | 40% REDUNDANCY |
|-----------------|------------|----------------|----------------|----------------|
| 200 | 1 | 2 | 2 | 2 |
| 500 | 1 | 2 | 2 | 2 |
| 1,000 | 2 | 3 | 3 | 3 |
| 2,000 | 4 | 5 | 5 | 6 |
| 5,000 | 10 | 11 | 12 | 14 |
| 10,000 | 20 | 22 | 24 | 28 |

Additional Instances of Opware Components and Load Balancing

If Opware SAS needs to support a larger operational environment, you might improve performance by installing additional instances of the following core components:

- Data Access Engine
- OS Provisioning Media Server
- Opware Command Center
- Opware Global Filesystem

Opware SAS does not support installing additional instances of the other components, such as the Command Engine or OS Provisioning Boot Server.

You can deploy a hardware load balancer for the servers that run additional instances of the Data Access Engine and Opware Command Center. Configure the load balancer for SSL session persistence (stickiness) with the least connections algorithm.

See the *Opware[®] SAS Administration Guide* for the steps to install an additional instance of an Opware SAS component.

Chapter 3: Pre-Installation Requirements

IN THIS CHAPTER

This section discusses the following topics:

- Operating System Requirements
- Network Requirements
- Patch Management Requirements
- Configuration Tracking Requirements
- Opware Global File System (OGFS) Requirements
- Time and Locale Requirements

Operating System Requirements

This section describes platform-specific requirements. For more information, see the “Hardware Requirements and Supported Operating Systems” section of the *Planning Deployments for Opware® SAS*.

Solaris Requirements

For Solaris, the Opware core servers must meet the following requirements.

Required Packages for Solaris

The following listing of a Solaris Jumpstart profile shows the required packages:

```
cluster    SUNWCreq
cluster    SUNWCpm delete
package    SUNWadmap add
package    SUNWadmc add
package    SUNWesu add
package    SUNWswmt add
package    SUNWtoo add
package    SUNWtoox add
package    SUNWadmfw add
package    SUNWlibC add
package    SUNWlibCx add
```

```
package SUNWinst add
package SUNWucbt add
package SUNWucbtX add
package SUNWscpu add
package SUNWscpux add
package SUNWtcsh add
package SUNWsacom add
package SUNWpnr add
```

Other Solaris Requirements

On the server where you will install the Opware Command Center component, you must install the J2SE Cluster Patches for Solaris. You can download these patches from the following location:

```
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches
/patch-access
```

On all core servers, verify that the Network File System (NFS) is configured and running.

Solaris 8 Requirements for Oracle 10g

When installing Oracle 10g by using the Opware Installer, you must install the following Solaris 8 operating system patches (with the version specified or higher):

```
108528-23: SunOS 5.8: kernel update patch
108652-66: X11 6.4.1: Xsun patch
108773-18: SunOS 5.8: IIIM and X I/O Method patch
108921-16: CDE 1.4: dtwm patch
108940-53: Motif 1.2.7 and 2.1.1: Runtime lib. patch for Solaris
8
108987-13: SunOS 5.8: Patch for patchadd and patchrm
108989-02: /usr/kernel/sys/acctctl & /.../exacctsys patch
108993-18: SunOS 5.8: LDAP2 client, libc, libthread...lib. patch
109147-24: SunOS 5.8: linker patch 110386-03: SunOS 5.8: RBAC
Feature Patch
111023-02: SunOS 5.8: /kernel/fs/mntfs and ... sparcv9/mntfs
111111-03: SunOS 5.8: /usr/bin/nawk patch
111308-03: SunOS 5.8: /usr/lib/libmtmalloc.so.1 patch
111310-01: SunOS 5.8: /usr/lib/libdhcpagent.so.1 patch
112396-02: SunOS 5.8: /usr/bin/fgrep patch
111721-04: SunOS 5.8: Math Library (libm) patch
112003-03: SunOS 5.8: Unable to load fontset in 64-bit Solaris 8
iso-1 or iso-15
112138-01: SunOS 5.8: usr/bin/domainname patch
```

Solaris 9 Requirements for Oracle 10g

When installing Oracle 10g by using the Opsware Installer, you must install the following Solaris 9 operating system patches (with the version specified or higher):

```
112233-11: SunOS 5.9: Kernel Patch
111722-04: SunOS 5.9: Math Library (libm) patch
```

Linux Requirements

For Linux, the Opsware core servers must meet the following requirements:

Required Packages for Linux

The following packages must be installed:

```
compat-db
compat-libstdc++
cpp
expat
gcc
glibc-devel
glibc-headers
glibc-kernheaders
kernel-source
libcap
libxml2-python
libstdc++-
libstdc++-devel
ncompress (contains uncompress utility)
nfs-utils
ntp
patch
patchutils
sharutils
strace
tcl
unzip
XFree86-libs
XFree86-libs-data
XFree86-Mesa-libGL
xinetd
zip
```

To verify that the `zip` package is installed, for example, enter the following command:

```
rpm -qa | grep zip
```

You can obtain the latest versions of these packages from the Red Hat errata web site.

Additional Linux Requirements for Oracle 10g

When installing Oracle 10g by using the Opware Installer, you must install the following Linux packages (with the version specified or higher):

```
make-3.79.1
glibc-2.3.2-95.20
compat-gcc-7.3-2.96.128
compat-gcc-c++-7.3-2.96.128
compat-libstdc++-devel-7.3-2.96.128
openmotif21-2.1.30-8
setarch-1.3-1
libaio-0.3.96-5
```

Packages on Linux that Must Be Uninstalled

If the Opware core server already has the following applications installed, you must uninstall them before running the Opware Installer.

```
samba
apache
rsync
httpd
tftp
dhcp
```

Existing versions of the `tftp` and `dhcp` packages cannot reside on the same server as the OS Provisioning Boot Server component, but they may reside on Opware core servers that do not have the OS Provisioning Boot Server component.

To remove the `rsync` package, for example, enter the following command:

```
rpm -e --nodeps rsync
```

Other Linux Requirements

For Linux systems, you must also perform the following tasks:

- Change the initial run level of the server to level 3 in the file `/etc/inittab`.
- If the server uses Integrated Drive Electronics (IDE) hard disks, enable Direct Memory Access (DMA) and some other advanced hard disk features to improve performance. Run the following script as root on the server, and then reboot the server:

```
cat > /etc/sysconfig/harddisks << EOF
USE_DMA=1
MULTIPLE_IO=16
EIDE_32BIT=3
LOOKAHEAD=1
EOF
```

Network Requirements

This section discusses the following network requirements within a facility, open ports required for core components, and name resolution requirements. These requirements must be met for both standalone and multimaster cores.

Network Requirements within a Facility

Before running the Opsware Installer, your environment must meet the following network requirements:

- The Opsware core servers must be on the same Local Area Network (LAN or VLAN).
- The Opsware core servers must have network connectivity to the servers that the Opsware core manages, and vice versa.
- The Opsware core servers cannot use the Network Information Service (NIS) for password and group databases. The Opsware components check for the existence of certain target accounts before creating them during installation.
- When using network storage for Opsware components, such as the Software Repository or Media Server, the network storage configuration must allow the root user to have write access over NFS to the directories where the components are to be installed.
- The speed and duplex mode of the NIC adapters of the Opsware core and managed servers must match the switch they are connected to. A mismatch causes poor network performance between the core and managed servers, making Opsware SAS unusable.

Open Ports

Table 3-1 shows the ports that must be open on firewalls that protect the Opsware core components. The Gateway ports listed are the default values, which can be changed during the installation.

Table 3-1: Open Ports on a Firewall Protecting an Opsware Core

| PORT | COMPONENT | PURPOSE |
|------------|------------------------|--|
| 80 (TCP) | Opsware Command Center | HTTP redirector |
| 443 (TCP) | Opsware Command Center | OCC Web UI, SAS Client, Opsware web services |
| 2001 (TCP) | Core Gateway | Inbound tunnels from other Gateways |

Table 3-1: Open Ports on a Firewall Protecting an Opsware Core (continued)

| PORT | COMPONENT | PURPOSE |
|------------------|--|---|
| 2222 (TCP) | Opsware Global File System | Global shell session from an SSH client |
| 3001 (TCP) | Agent Gateway | Inbound Agent connections |
| 7580, 7581 (TCP) | Model Repository Multimaster Component | TIBCO Rendezvous web client |
| 8017 (UDP, TCP) | Agent Gateway | Interface to the Build Manager |
| 8080 (TCP) | Opsware Command Center | OGFS Gateway for the OCC Client |

Table 3-2 shows the ports for the OS provisioning components that are accessed by servers during the provisioning process. (In Opsware SAS, provisioning refers to the installation of an operating system on a server.)

Table 3-2: Open Ports for the OS Provisioning Components

| PORT | COMPONENT | SERVICE |
|-----------------|---------------------------|---|
| 67 (UDP) | Boot Server | DHCP |
| 69 (UDP) | Boot Server | TFTP |
| 111 (UDP, TCP) | Boot Server, Media Server | RPC (<code>portmapper</code>), required for NFS |
| Dynamic* | Boot Server, Media Server | <code>rpc.mountd</code> , required for NFS |
| 2049 (UDP, TCP) | Boot Server, Media Server | NFS |

* The `rpc.mountd` process runs on a dynamic port and is not fixed. Therefore, if a firewall is in place, it must be an application layer firewall that can understand the RPC request that the client uses to locate the port for `mountd`. The firewall must dynamically open that port.

Table 3-3 shows the ports that must be open on managed servers so that Opsware core servers can connect to managed servers.

Table 3-3: Open Ports on Managed Servers

| PORT | COMPONENT |
|------------|---------------|
| 1002 (TCP) | Opsware Agent |

Host and Service Name Resolution Requirements

Opsware SAS must be able to resolve Opsware server host names and service names to IP addresses through configuration of DNS or `/etc/hosts`.

Previous Releases

If you are installing Opsware components on servers where a previous release of Opsware SAS was installed (for example, 4.0), you must verify that the host names and service names resolve correctly as noted in this section.

Opsware Core Servers and Name Resolution

An Opsware core server must be able to resolve the fully qualified host name of itself and any other Opsware core server. (A fully qualified name includes the subdomain, for example, `myhost.acct.buzzcorp.com`.) Enter the `hostname` command and verify that it displays the fully qualified name.

Additionally, an Opsware core server must be able to resolve both the fully qualified and unqualified names of the Opsware services. (Each service name represents an Opsware component.) For example, both `truth` (unqualified) and `truth.acct.buzzcorp.com` (fully qualified) must resolve to the IP address of the server containing the Model Repository. The list of fully qualified names of the Opsware services follows:

- `truth.subdomain` - Model Repository
- `way.subdomain` - Command Engine
- `spin.subdomain` - Data Access Engine
- `theword.subdomain` - Software Repository
- `twist.subdomain` - Web Services Data Access Engine
- `occ.subdomain` - Opsware Command Center
- `buildmgr.subdomain` - OS Provisioning Build Manager

- `wordcache.subdomain` - Software Repository Multimaster Component (The name `wordcache` must resolve to the core server running the Software Repository.)

The Software Repository server must be able to resolve the IP address to the host name of the OGFS server. To enable this reverse lookup, configure DNS.

DHCP Proxying

If network provisioning occurs on a separate network from the Opsware core components, you must set up DHCP proxying (for example, with Cisco IP Helper) to the DHCP server. If you set up DHCP proxying, the server/router performing the DHCP proxying must be the router for the network so that PXE will function correctly in the Opsware OS Provisioning Feature.

The Opsware Boot Server component includes a DHCP server, but does not include a DHCP proxy. You configure the DHCP server after installation by using the Opsware DHCP Network Configuration Tool. See *DHCP Configuration for OS Provisioning* in Chapter 7, on page 117.

DMZ Network



The Boot Server and Media Server run various services (such as portmapper and `rpc.mountd`) that have been susceptible to network attacks. Opware Inc. recommends that you segregate the OS Provisioning Boot Server and Media Server components onto their own DMZ network. When you segregate these components, the ports listed previously) should be opened to the DMZ network from the installation client network. Additionally, the Boot Server and Media Server should have all vendor-recommended security patches applied.

Patch Management Requirements

You must obtain several files from Microsoft and copy them to a directory that is accessible by the Opware Installer. When you install the Opware Software Repository, the Opware Installer prompts you for the directory name.

Perform the following steps:

1 Obtain the following Microsoft Base Security Analyzer (MBSA) 1.2.1 files:

- `qchain.exe`

The `qchain.exe` utility is a command-line program that chains hotfixes together.

Download the package containing `qchain.exe` from the following URL:

<http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=3C64D889-74F1-490B-A2FB-F15671A3B60C&displaylang=en>

Install the package on a Windows machine and locate the `qchain.exe` file.

- `mssecure.cab`

The `mssecure.cab` file contains the Microsoft patch database. Download `mssecure.cab` from the following URL:

<http://go.microsoft.com/fwlink/?LinkId=18922>

- `mbsacli.exe`

Packaged with the MBSA 1.2.1 software, the `mbsacli.exe` utility is a command-line program that performs security scans. Download MBSA 1.2.1 from the following URL:

```
http://download.microsoft.com/download/9/0/7/90769f0c-
c025-48bf-a9c7-60072d0cb717/MBSASetup-EN.msi
```

After the download, on a Windows machine run `MBSASetup-EN.msi` to install MBSA 1.2.1.

In the directory where you installed MBSA 1.2.1, locate the `mbascli.exe` file. By default, the file is installed here:

```
%program files%\Microsoft Baseline Security
Analyzer\mbascli.exe
```

- 2 Copy the MBSA 1.2.1 files you obtained in the preceding step to a directory that is accessible by the server where you will install the Opware Software Repository. For example, you might copy the files to the following directory:

```
/home/win_util
```

The files that you want to copy are:

```
qchain.exe
mssecure.cab
mbsacli.exe
```

- 3 Obtain the following Microsoft Base Security Analyzer (MBSA) 2.0 files:

- `wsusscan.cab`

The `wsusscan.cab` file contains the Microsoft patch database. Download `wsusscan.cab` from the following URL:

```
http://go.microsoft.com/fwlink/?LinkId=39043
```

- `WindowsUpdateAgent20-x86.exe`

The `WindowsUpdateAgent20-x86.exe` file is required by the `mbsacli20.exe` utility. Download `WindowsUpdateAgent20-x86.exe` from the following URL:

```
http://go.microsoft.com/fwlink/?LinkId=43264
```

- `WindowsUpdateAgent20-x64.exe`

The `WindowsUpdateAgent20-x64.exe` file is required by the `mbsacli20.exe` utility. Download `WindowsUpdateAgent20-x64.exe` from the following URL:

```
http://go.microsoft.com/fwlink/?LinkId=43265
```

- `mbsacli20.exe`

This utility is packaged with the MBSA 2.0 software as `mbsacli.exe`. In a later step, you will copy `mbsacli.exe` to `mbsacli20.exe`.

The download files for MBSA 1.2.1 and MBSA 2.0 have the same name: MBSASetup-EN.msi. Before you download MBSA 2.0, rename the MBSASetup-EN.msi file you downloaded for MBSA 1.2.1.

Download MBSA 2.0 from the following URL:

```
http://www.microsoft.com/downloads/
info.aspx?na=208&p=2&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=4B4ABA06-B5F9-4DAD-BE9D-7B51EC2E5AC9&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2f3%2ff%2fd%2f3fd1a09d-af15-4ab7-a554-0ac6c1e76c16%2fMBSASetup-EN.msi
```

After the download, on a Windows machine run MBSASetup-EN.msi to install MBSA 2.0. Do not overwrite the MBSA 1.2.1 installation. The default installation directories are different.

In the directory where you installed MBSA 2.0, locate the `mbsacli.exe` file. By default, the file is installed here:

```
%program files%\Microsoft Baseline Security Analyzer
2\mbsacli.exe
```

- `wusscan.dll`

The `wusscan.dll` file is in the directory where you installed MBSA 2.0. By default, the file is here:

```
%program files%\Microsoft Baseline Security Analyzer
2\wusscan.dll
```

- 4 Copy the MBSA 2.0 `mbsacli.exe` file to `mbsacli20.exe` in the directory where you copied the files in step 2.

Do *not* overwrite the MBSA 1.2.1 `mbsacli.exe` file you copied in step 2.

- 5 Copy the other three files you downloaded in step 3 to the directory where you copied the files in step 2. These other three files are:

```
wsusscan.cab
WindowsUpdateAgent20-x86.exe
wusscan.dll
```

- 6 Verify that the destination directory contains the following files:

```
mbsacli.exe
mbsacli20.exe
mssecure.cab
qchain.exe
WindowsUpdateAgent20-x86.exe
wsusscan.cab
wusscan.dll
```

- 7 Write down the name of the directory containing the files listed in the preceding step. When you install the Opware Software Repository, you are prompted for the directory name. The Opware Installer prompt is `windows_util_loc`.

During Opware Agent installation, the files you obtained from Microsoft are downloaded from the Opware Software Repository to the appropriate Windows servers. If newer versions of the files are uploaded to the Opware Software Repository, they are downloaded to the managed servers during software registration.

Configuration Tracking Requirements

When you run the Opware Configuration Tracking feature in a facility, you must create a separate partition on the server running the Software Repository for the following Configuration Tracking directory:

```
/cust/word/<facility-name>/acsbar
```

The Configuration Tracking feature uses this directory to store the backup versions of tracked configuration files and databases.

Opware Global File System (OGFS) Requirements

This section discusses requirements of the OGFS.

OGFS Store and Audit Hosts

When you run the Opware Installer interviewer in advanced mode, you can specify values for the `ogfs.store.host` and `ogfs.audit.host` parameters. (See “Opware Global File System Prompts” on page 94.) If you set either of these parameters to a host that runs neither the OGFS nor the Software repository, then perform the following steps on the host where you will install the OGFS:

- 1 With `mkdir`, create the directories that you specified for the `ogfs.store.path` and `ogfs.audit.path` parameters.
- 2 With a text editor, modify the `/etc/exports` file. For example:

```
# Begin Opware ogfs exports
  /cust/ogfs/store *(ro) 1.2.3.4(rw,no_root_squash)
  /cust/ogfs/audit *(ro) 1.2.3.4(rw,no_root_squash)
# End Opware ogfs exports
```
- 3 Run the following command:

```
exportfs -a
```

Name Service Caching Daemon (nscd) and OGFS

If the Name Service Caching Daemon (`nscd`) runs on the same server as the OGFS, then users cannot open a global shell session with a direct `ssh` connection. If `nscd` is running on the OGFS server, the Opsware Installer turns it off and runs the `chkconfig nscd off` command to prevent it from starting after a reboot. No action by you is required.

Time and Locale Requirements

This section discusses the time and locale requirements for core servers.

Core Time Requirements

Opsware core servers (either standalone or multimaster) and Opsware Satellite servers must meet the following requirements. These time requirements do not apply to managed servers (that is, servers with Opsware Agents).

- Opsware core servers must maintain synchronized clocks. For example, you can synchronize the system clocks with an external server that uses NTP (Network Time Protocol) services.
- Opsware core servers must have their time zone set to Coordinated Universal Time (UTC).

On Linux servers, to configure the time zone, perform the following steps:

- Copy or link `/usr/share/zoneinfo/UTC` to `/etc/localtime`.
- Make sure that `/etc/sysconfig/clock` contains the following lines:

```
ZONE="UTC"  
UTC=true
```

On Solaris servers, to configure the time zone, verify that `/etc/TIMEZONE` contains the following line:

```
TZ=UTC
```

Locale Requirements

The core servers with the Model Repository and the Software Repository must have the `en_US.UTF-8` locale installed. To display data from managed servers in various locales, the core server with the Opware Global File System (OGFS) must have those locales installed.

Chapter 4: Installation Overview and Checklists

IN THIS CHAPTER

This section discusses the following topics:

- Types of Opware SAS Installations
- Opware Core Installation Process Flow
- Checklists

Types of Opware SAS Installations

There are three basic types of Opware SAS installations: standalone, multimaster, and satellite.

- **Standalone:** A standalone core does not communicate or exchange information with other cores. A standalone core manages servers in a single facility. (Optionally, a standalone core can also manage servers in remote facilities installed with Opware Satellites.) A core contains all components of Opware SAS, except for the Opware Agents, which run on the servers managed by the core.
- **Multimaster:** A multimaster core exchanges information with other cores. This collection of cores is called a multimaster mesh. With a multimaster mesh, you can centralize the management of several facilities but still get the performance benefits of having a local copy of key Opware SAS data at each facility.
- **Satellite:** Installed in a remote facility, an Opware Satellite provides 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.



This guide uses the term facility to refer to the collection of servers and devices that reside in a single physical location. A facility can be all or part of a data center, server room, or computer lab. Each Opware core or Satellite is associated with a specific facility.

Opware Core Installation Process Flow

Figure 4-1 shows the overall process of an Opware core installation. The main phases of the installation process follow:

- 1 Planning:** Decide which type of Opware SAS installation is appropriate for your site and what hardware needs to be procured. At the end of this phase, you may follow the instructions in this installation guide.

See Chapter 1, “Opware SAS Architecture” on page 17 of this guide for more information.

See Chapter 2, “Supported Operating Systems and Hardware Requirements” on page 39 of this guide for more information.

- 2 Pre-installation Requirements:** At this point, you have the necessary hardware in place and you are ready to install an Opware core. In this phase, you perform hands-on administrative tasks such as resolving host names, opening ports, and installing the necessary OS utilities or patches.

See Chapter 3, “Pre-Installation Requirements” on page 49 of this guide for more information.

- 3 Pre-requisite Information for Installer Interview:** Gather information for the Opware Installer interview, which prompts you for information about the core and your operational environment. This information includes the name of the facility to be managed by the core, the authorization domain, as well as information about the Oracle database that underlies the Opware Model Repository.

At the end of this phase, you are ready to run the Opware Installer to perform one of the following three types of installations.

See Chapter 5, “Prerequisite Information for the Installer Interview” on page 75 of this guide for more information.

- 4 Perform Installation:** Run the Opware Installer, complete the interview, and install one of the following types of Opware SAS cores or Opware Satellite:

- **Standalone Core Installation:** Run the Opware Installer for the interview and then create the core.

See Chapter 6, “Opware Standalone Installation” on page 101 of this guide for more information.

- **Multimaster Core Installation:** Run the Opware Installer for the interview and then add a core to a multimaster mesh.

See Chapter 8, “Opware Multimaster Installation” on page 133 of this guide.Or

- **Satellite Realm Installation:** Run the Opware Installer for the interview and create an Opware Satellite in a remote facility.

See Chapter 9, “Opware Satellite Installation” on page 151 of this guide for more information.

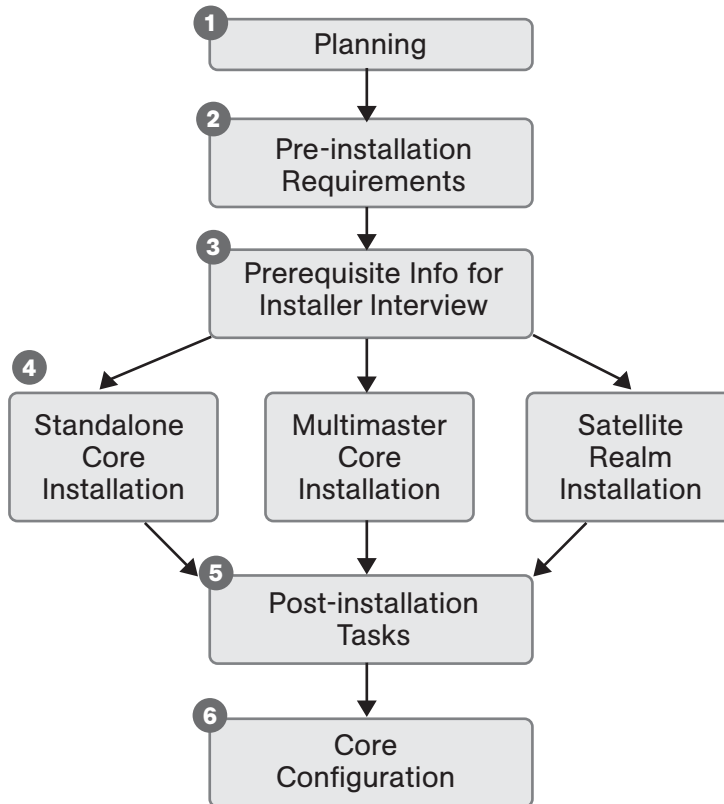
- 5 Post-installation Tasks:** Perform hands-on administrative tasks such as configuring the DHCP server in preparation for Opware OS Provisioning. At the end of this phase, the newly installed Opware core is up and running.

See Chapter 7, “Post-Installation Tasks” on page 111 of this guide.

- 6 Core Configuration:** Configure Opware SAS, performing tasks such as creating Opware users, groups, and the software tree. At the end of this phase, Opware SAS is ready for operational use by system administrators.

See the *Opware[®] SAS Administration Guide* for more information.

Figure 4-1: Opware Core Installation Process Flow



Checklists

This section discusses the following topics:

- Overall Planning Checklist
- Specific Core Planning Checklist
- Specific Core Requirements Checklist
- Pre-Installation Tasks Checklist
- Post-Installation Tasks Checklist

Overall Planning Checklist

The following checklist summarizes decisions regarding the overall design of your Opsware SAS installation.

Table 4-4: Overall Planning Checklist

| OVERALL PLANNING ITEM | ANSWER |
|---|--------|
| How many facilities (data centers) will you manage Opsware SAS? | |
| In each of these facilities, how many servers will you manage with Opsware SAS? | |
| What is your naming convention for the Opsware facility names? (For example, you might use building or city names.) | |
| Have you taken an inventory of the operating systems and applications on the servers that you will manage with Opsware SAS? | |
| Which operating systems will you provision (install) with Opsware SAS? | |
| What applications will you provision (install) with Opsware SAS? | |
| Which Opsware SAS features will you use? | |
| What is your schedule for installing Opsware SAS core and for installing agents on the servers to be managed? | |
| Which of the following Opsware SAS architectures have you chosen? <ul style="list-style-type: none"> • Standalone • Multimaster mesh • Satellite | |

Table 4-4: Overall Planning Checklist

| OVERALL PLANNING ITEM | ANSWER |
|---|--------|
| If you will be using multimaster mesh, how fast is the network connection between the Opsware cores? | |
| How many cores will you install? | |
| For each core, in which facility will it reside? | |
| How many Opsware Satellites will you install? | |
| For each Satellite, in which remote facility will it reside? | |
| Which cores will the Satellite communicate with? | |
| How fast is the network connection between the Satellite and the core? | |
| Have you drawn a diagram showing the hosts that will run the Opsware core components? If applicable, the diagram should show the network connectivity between multimaster cores and between cores and Satellites. | |

Specific Core Planning Checklist

The following checklist summarizes design decisions for a specific Opsware core installation.

Table 4-5: Specific Core Planning Checklist

| SPECIFIC CORE PLANNING ITEM | ANSWER |
|---|--------|
| In which facility will this core reside? | |
| What will be the facility name? | |
| For the first core, what will be the facility ID and the default customer name? | |

Table 4-5: Specific Core Planning Checklist

| SPECIFIC CORE PLANNING ITEM | ANSWER |
|--|--------|
| How many servers will this Opsware core manage? | |
| Will you distribute the Opsware core components across multiple servers? | |
| What are the host names of the servers on which the core components will be installed? | |
| For a multiple-server core, have you drawn a diagram that shows which components will run on which servers? | |
| For a multimaster mesh, will you be using an Opsware Software Repository Replicator? | |
| <p>For a multiple-server core, will you have multiple instances of the following Opsware components?</p> <ul style="list-style-type: none"> • Data Access Engine • Opsware Command Center (OCC) • Media Server • Global File System Server | |
| <p>Will you deploy a load balancer on multiple instances of the following Opsware components?</p> <ul style="list-style-type: none"> • Data Access Engine • Opsware Command Center (OCC) | |
| <p>Will you install the following Opsware components into their own DMZ network?</p> <ul style="list-style-type: none"> • OS Provisioning Boot Server • OS Provisioning Media Server | |

Table 4-5: Specific Core Planning Checklist

| SPECIFIC CORE PLANNING ITEM | ANSWER |
|---|--------|
| Do you have the necessary licenses for Oracle? (The Opware Model Repository uses an Oracle database.) | |
| Have you written your backup and recovery plan for the servers running Opware SAS? | |
| Have you contacted your database administrator (DBA)? Your DBA will need to monitor the Oracle database when it goes into production. | |
| Have you contacted your network administrator? He or she will need to setup host name resolution (/etc/hosts, DNS) before the installation and will run a DHCP configuration tool after the installation. | |
| Which version of Opware SAS are you installing? | |

Specific Core Requirements Checklist

The following checklist summarizes the technical requirements that must be met before Opware core installation.

Table 4-6: Specific Core Requirements Checklist

| REQUIREMENT | ANSWER |
|--|--------|
| Have the hardware servers on which you will install the Opware core components (core servers) been racked and stacked? | |
| Do you have root access to the core servers? | |
| Will you be able to mount Opware SAS DVDs and copy their contents to the core servers? | |

Table 4-6: Specific Core Requirements Checklist

| REQUIREMENT | ANSWER |
|--|--------|
| Are the core servers running a supported operating system? | |
| Do the core servers meet the CPU requirements? | |
| Do the core servers meet the memory requirements? | |
| Do the core servers meet the disk space requirements? | |
| Are the servers for an individual core on the same LAN or VLAN? (Multimaster cores must be on separate VLANs.) | |
| Do the core servers have network connectivity to the servers they will manage? | |
| Have you verified that Network Information System (NIS) is <i>not</i> running on the core servers? | |
| If you will be using the Network File System (NFS) for Opsware components, such as the Software Repository or Media Server, does the root user have write access over NFS to the directories where the components are to be installed? | |
| Does the link speed and duplex of core and managed servers match the switch to which they are connected? | |
| Are the necessary TCP ports open on the core and managed servers? | |

Pre-Installation Tasks Checklist

The following checklist summarizes the hands-on tasks you must perform before installing an Opware core.

Table 4-7: Pre-Installation Tasks Checklist

| PRE-INSTALLATION TASK | TASK COMPLETED? |
|---|-----------------|
| For the servers that will run the Opware core components (core servers), perform the specific tasks for Linux and Solaris described in the section "Operating System Requirements" on page 49 (<i>Opware® SAS Deployment and Installation Guide</i>). | |
| Set up the host name resolution (/etc/hosts or DNS) for the core servers. | |
| If network provisioning occurs on a separate network from the Opware core components, you must set up DHCP proxying. | |
| Obtain <code>qchain.exe</code> , <code>mbsaccli.exe</code> , and <code>mssecure.cab</code> from Microsoft and copy them to a location on your network that is accessible by the Opware installer. | |
| Synchronize the system clocks on the core servers with an external Network Time Protocol (NTP) service. | |
| For a multimaster mesh, see the section "Prerequisites for a Multimaster Installation" on page 135 (<i>Opware® SAS Deployment and Installation Guide</i>). | |
| Verify that you have followed the instructions in Chapter 5, "Prerequisite Information for the Installer Interview" (<i>Opware® SAS Deployment and Installation Guide</i>). | |

Post-Installation Tasks Checklist

The following checklist summarizes the hands-on tasks you must perform after installing an Opware core. For more information, see the “Post-Installation Tasks” chapter of the *Opware® SAS Deployment and Installation Guide*.

Table 4-8: Post-Installation Tasks Checklist

| POST-INSTALLATION TASK | TASK COMPLETED? |
|---|-----------------|
| Install the Windows Agent Deployment Helper. | |
| Configure DHCP for Opware OS Provisioning. You may use the DHCP server included with Opware SAS or an external DHCP server. | |
| For Windows OS provisioning, the host name <code>buildmgr</code> should resolve on Windows installation clients. | |
| For Patch Management on Windows NT or 2000, create a silent-installable version of IE 6.0 or later. | |
| Multimaster mesh: Associate customers with the new facility. | |
| Multimaster mesh: Update the group permissions for the new facility. | |
| Multimaster mesh: Verify that the multimaster transaction traffic is flowing between the cores. | |

Chapter 5: Prerequisite Information for the Installer Interview

IN THIS CHAPTER

This section discusses the following topics:

- Required Information for Running the Installer Interview
- Opsware Installer

Required Information for Running the Installer Interview

The Opsware Installer interview prompts you for information about your environment that it saves in a response file. After the interview, the Opsware Installer reads the response file when it installs an Opsware core component onto a server.

Before you run the Installer interview, you must gather the information that you will enter for the interview prompts. Examples of this information are: the password for the Oracle `opsware_admin` user, the Opsware facility name for the core, and the Opsware authorization domain.

The Opsware Installer prompts you for a mode, either simple or advanced. In the simple mode, the Installer interview prompts you for fewer parameters.

The tables that follow list the various prompts that you will respond to when running the Installer interview. In the tables, prompts required only for the installation of a multimaster core are indicated by the word **Multimaster** (in bold font). Prompts required only for the advanced mode are denoted by the word **Advanced**.

Model Repository Prompts

The Model Repository is the database that stores information about the hardware and software deployed in the operational environment. Most of the Model Repository prompts are for a standalone Opware core. However, for multimaster mesh cores, you need to provide some additional information.

Table 5-1: Model Repository Prompts

| PROMPT | DESCRIPTION |
|---|---|
| <p>Enter the service name (aka TNS name) of the Model Repository instance.</p> <p>(Parameter: truth.servicename)</p> | <p>Specifies the service name, also known as the alias, for the Model Repository.</p> <p>The service name can be determined by looking in the <code>tnsnames.ora</code> file on the Model Repository instance. The service name is the value before the first equals sign (=) in the file. The location of this file can vary, so check with your DBA if you are not sure where to look.</p> <p>Source: The DBA who created the Oracle database.</p> <p>Example: <code>truth.opsware.com</code></p> |
| <p>Enter the service name (aka TNS name) of the Model Repository instance that you will be installing in the new facility.</p> <p>(Parameter: slaveTruth.servicename)</p> | <p>Multimaster: Specifies the service name, also known as the alias, for the Model Repository of the target core.</p> <p>The service name can be determined by looking in the <code>tnsnames.ora</code> file on the Model Repository instance. The location of this file can vary, so check with your DBA if you are not sure where to look.</p> <p>Source: The DBA who created the Oracle database.</p> <p>Example: <code>truth02.opsware.com</code></p> |

Table 5-1: Model Repository Prompts (continued)

| PROMPT | DESCRIPTION |
|--|--|
| <p>Enter the SID of the Oracle instance that contains the Data Model Repository.</p> <p>(Parameter: <code>truth.sid</code>)</p> | <p>Multimaster: Specifies the database system ID (SID) that was set when Oracle was installed on the server where the Model Repository is installed.</p> <p>You can find out the SID by looking at the <code>tnsnames.ora</code> file. The location of this file can vary, so check with your DBA if you are not sure where to look.</p> <p>Source: The DBA who created the Oracle database.</p> <p>Example: <code>DTC05</code></p> |
| <p>Enter the path of the Oracle home.</p> <p>(Parameter: <code>truth.orahome</code>)</p> | <p>Specifies the base directory of the Oracle installation that was set when Oracle was installed.</p> <p>You can determine the Oracle home directory by logging in as the <code>oracle</code> user on the Model Repository server, and checking the value of the <code>\$ORACLE_HOME</code> environment variable. (For a remote database, this parameter refers to the installation of Oracle Client on the Model Repository server.)</p> <p>Source: The DBA who created the Oracle database.</p> <p>Example: <code>/cust/oracle/product/9.1</code></p> |
| <p>Enter the path to the TNS admin directory (where the <code>tnsnames.ora</code> file resides).</p> <p>(Parameter: <code>truth.tnsdir</code>)</p> | <p>Specifies the directory that contains the <code>tnsnames.ora</code> file. The location of the <code>tnsnames.ora</code> file can vary, so check with your DBA if you are not sure where to look.</p> <p>Source: The DBA who created the Oracle database.</p> <p>Example: <code>/var/opt/oracle</code></p> |

Table 5-1: Model Repository Prompts (continued)

| PROMPT | DESCRIPTION |
|---|---|
| <p>Enter the full path to the directory where the export file will be saved. (Parameter: <code>truth.dest</code>)</p> | <p>Multimaster: Specifies the directory where the database export file will be saved. This directory must exist on the Model Repository server in the source facility.</p> <p>When adding a facility to a multimaster mesh, you must export the Model Repository from the source facility, then copy it to the destination facility.</p> <p>Source: Arbitrary. (However, you must create the directory on the server before you run the Opware Installer.)</p> <p>Example: <code>/export/home/core1</code></p> |
| <p>Enter the full path to the directory that contains the export file. (Parameter: <code>truth.sourcePath</code>)</p> | <p>Multimaster: Specifies the directory on the Model Repository server in the destination facility where the export data file was copied from the source facility.</p> <p>When adding a facility to a multimaster mesh, you must export the Model Repository data from the source facility, then copy it to the destination facility.</p> <p>Source: Arbitrary. (However, the directory must exist on the server and contain the database export file before you run the Opware Installer on that server.)</p> <p>Example: <code>/export/home/core2</code></p> |
| <p>Please enter the IP address of the device where you are planning to install the Model Repository in the new facility. (Parameter: <code>slaveTruth.truthIP</code>)</p> | <p>Multimaster: Specifies the IP address of the host on which you will install the Model Repository for the new target core.</p> <p>Source: Arbitrary.</p> <p>Example: <code>192.168.165.242</code></p> |

Table 5-1: Model Repository Prompts (continued)

| PROMPT | DESCRIPTION |
|---|---|
| Please enter the IP address of the device where you are planning to install the Multimaster Infrastructure Components (vault). (Parameter: <code>slaveTruth.vaultIP</code>) | Multimaster: Specifies the IP address of the host on which you will install the Multimaster Infrastructure Components for the core. Source: Arbitrary. Example: <code>192.168.165.242</code> |

Database (Model Repository) Password Prompts

To ensure a secure installation of Opware SAS, the Opware Installer prompts you to set passwords for numerous Oracle user accounts that the Opware components use to interact with one another. The passwords must meet standard Oracle criteria, as follows:

- The password cannot contain an Oracle reserved word (see Oracle's documentation for a full list).
- The password must be between 1 and 30 characters long.
- The password must start with a letter and use only alphanumeric and underscore (`_`) characters.

Table 5-2: Database Password Prompts

| PROMPT | DESCRIPTION |
|--|--|
| Enter database password for the <code>opsware_admin</code> user. (Parameter: <code>truth.oaPwd</code>) | Specifies the <code>opsware_admin</code> password created by your database administrator. <code>opsware_admin</code> is an Oracle user that the Opware Installer uses during installation to perform certain functions. Source: This must be the password that your DBA set for the <code>opsware_admin</code> user when setting up the Oracle instance on the server where you will install the Model Repository. |

Table 5-2: Database Password Prompts (continued)

| PROMPT | DESCRIPTION |
|--|---|
| <p>Enter database password for the lcrep user.</p> <p>(Parameter: <code>truth.lcrepPwd</code>)</p> | <p>Advanced: Sets the password for the <code>lcrep</code> database user.</p> <p>The Opware Installer automatically creates an Oracle user <code>lcrep</code>, which Opware SAS uses internally for running multimaster replication between Opware cores.</p> <p>Source: Arbitrary. (However, must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |
| <p>Enter database password for the gadmin user.</p> <p>(Parameter: <code>truth.gcPwd</code>)</p> | <p>Sets the password for the <code>gadmin</code> database user.</p> <p>The Opware Installer automatically creates an Oracle user <code>gadmin</code>, which Opware SAS uses internally for removing old data from certain tables (referred to as the garbage collection process).</p> <p>Source: Arbitrary. (However, must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |
| <p>Enter the database password for the truth user.</p> <p>(Parameter: <code>truth.truthPwd</code>)</p> | <p>Advanced: Sets the password for the <code>he truth</code> user.</p> <p>The Opware Installer automatically creates this Oracle user, which is the main schema owner for the Model Repository.</p> <p>Source: Arbitrary. (However, must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |

Table 5-2: Database Password Prompts (continued)

| PROMPT | DESCRIPTION |
|--|--|
| <p>Enter the database password for the spin user.</p> <p>(Parameter: <code>truth.spinPwd</code>)</p> | <p>Advanced: Sets the password for the <code>spin</code> user.</p> <p>The Opsware Installer automatically creates this database user.</p> <p>Source: Arbitrary. (However, it must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> <p>Note: Passwords for the <code>spin</code> user must be the same across all the cores in the mesh.</p> |
| <p>Enter the database password for the twist user.</p> <p>(Parameter: <code>truth.twistPwd</code>)</p> | <p>Advanced: Sets the password for the <code>twist</code> user.</p> <p>The Opsware Installer automatically creates this user.</p> <p>Source: Arbitrary. (However, it must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |
| <p>Enter the database password for the vault user.</p> <p>(Parameter: <code>truth.vaultPwd</code>)</p> | <p>Multimaster: Sets the Model Repository, Multimaster Component password. This prompt only appears when installing Opsware SAS in multimaster mode.</p> <p>The Opsware Installer automatically creates the <code>vault</code> user.</p> <p>The Model Repository, Multimaster Component propagates and synchronizes changes from each Model Repository database to all other Model Repository databases.</p> <p>Source: Arbitrary. (However, it must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |

Table 5-2: Database Password Prompts (continued)

| PROMPT | DESCRIPTION |
|--|---|
| <p>Enter the database password for the public views user.</p> <p>(Parameter: <code>truth.pubViewsPwd</code>)</p> | <p>Advanced: Sets the password for the <code>public_views</code> user, which Opware SAS uses for the Data Center Intelligence (DCI) module (server reporting). The DCI module uses this password when connecting with the Model Repository. The Opware Installer automatically creates the public views user.</p> <p>If you are using Brio, Crystal Reports, or other data reporting tools with the DCI module, you are asked for the database user password when you log into those applications so that you have read-only access to the Model Repository data.</p> <p>Source: Arbitrary. (However, it must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |
| <p>Enter the database password for the AAA user.</p> <p>(Parameter: <code>truth.aaaPwd</code>)</p> | <p>Advanced: Sets the password for the AAA user, which Opware SAS uses for the Access, Authentication, and Authorization (AAA) feature. The Opware Installer automatically creates the AAA user.</p> <p>Source: Arbitrary. (However, it must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |
| <p>Please enter the password to use for DCML exchange tool user.</p> <p>(Parameter: <code>truth.detuserpwd</code>)</p> | <p>Advanced: Sets the password for the <code>DETUSER</code>, which Opware SAS uses for the DCML Exchange Tool (DET). The Opware Installer automatically creates the <code>DETUSER</code>.</p> <p>Source: Arbitrary. (However, it must meet the requirements for Oracle passwords.)</p> <p>Example: <code>x145_pwd03</code></p> |

Opware Component Password Prompts

This section lists the password prompts for the components other than the Model Repository.



In a multimaster mesh, the following passwords set during the Opware Installer interview must be the same in all cores belonging to the mesh.

Table 5-3: Component User and Password Prompts

| PROMPT | DESCRIPTION |
|--|--|
| Enter the password for Build Manager user. (Parameter: <code>twist.buildmgr.passwd</code>) | <p>Advanced: Sets the password for the <code>buildmgr</code> user that the <code>buildmgr</code> process will use when connecting to and authenticating with the Web Services Data Access Engine. The Opware Installer automatically creates this user.</p> <p>The password cannot contain spaces or a forward slash (/).</p> <p>Source: Arbitrary.</p> <p>Example: <code>x145_pwd03</code></p> |
| Enter the password for Integration user. (Parameter: <code>twist.integration.passwd</code>) | <p>Advanced: Sets the password for the <code>integration</code> user that a customer can use to access the SOAP APIs on the Web Services Data Access Engine. The Opware Installer automatically creates the <code>integration</code> user.</p> <p>The password cannot contain a forward slash (/).</p> <p>Source: Arbitrary.</p> <p>Example: <code>x145_pwd03</code></p> |

Table 5-3: Component User and Password Prompts (continued)

| PROMPT | DESCRIPTION |
|--|--|
| <p>Enter the password to decrypt cryptographic material.</p> <p>(Parameter: <code>decrypt_passwd</code>)</p> | <p>Sets the password to use for decrypting cryptographic material. It cannot contain any spaces. The password must be between 4 and 20 characters long.</p> <p>This password must be the same across all Opware cores in a multimaster mesh.</p> <p>Source: Arbitrary.</p> <p>Example: <code>x145_pwd03</code></p> |
| <p>Enter the password to use for admin entry.</p> <p>(Parameter: <code>cast.admin_pwd</code>)</p> | <p>Sets the password for the Opware <code>admin</code> user. The password cannot contain any spaces. The Opware Installer automatically creates the <code>admin</code> user.</p> <p>When you log into the Opware Command Center in the facility, you log in as the <code>admin</code> user supply the password you provide at this prompt.</p> <p>In general, you will <i>not</i> need to log into the directory manager (Netscape Directory Server) by using this user and password unless you need to troubleshoot directory issues.</p> <p>Source: Arbitrary.</p> <p>Example: <code>x145_pwd03</code></p> |

Facility Prompts

A facility refers to the collection of servers that a single Opsware core manages. If you are performing a standalone core installation, your deployment is made up of a single facility. Multimaster installations, however, make up two or more facilities: one facility for each core that you install.

Table 5-4: Facility Prompts

| PROMPT | DESCRIPTION |
|--|--|
| Enter the authorization domain (uppercase). (Parameter: <code>truth.authDom</code>) | Sets the authorization domain for the initial (default) customer. This value is usually the same as the domain name. It must be uppercase, less than 50 characters, and in domain name format. You must use the same value for every Opsware core in your multimaster mesh. The Opsware Installer only prompts you for this value when you are installing your first, standalone Opsware core. Source: Arbitrary. Example: <code>XYZ.COM</code> |
| Enter the subdomain for this facility (lowercase, no spaces). (Parameter: <code>truth.dcSubDom</code>) | Specifies the fully-qualified DNS subdomain where the Opsware core is deployed. This value must be unique for each core in the multimaster mesh. The value is based on the VLAN for the facility in which you are installing the Opsware core. It must be lowercase, less than 50 characters, and in subdomain format. Source: Your network administrator. Example: <code>dc1.opsware.com</code> |

Table 5-4: Facility Prompts (continued)

| PROMPT | DESCRIPTION |
|---|---|
| <p>Please enter the subdomain for the facility you are about to create (lowercase, no spaces).</p> <p>(Parameter: <code>slaveTruth.dcSubDom</code>)</p> | <p>Multimaster. Specifies the fully-qualified DNS subdomain where the target core is deployed.</p> <p>This value must be unique for each core in the multimaster mesh. The value is based on the VLAN for the facility in which you are installing the target core.</p> <p>It must be lowercase, less than 50 characters, and in subdomain format.</p> <p>Source: Your network administrator.</p> <p>Example: <code>dc2.opsware.com</code></p> |
| <p>Enter the facility short name (uppercase, no spaces).</p> <p>(Parameter: <code>truth.dcNm</code>)</p> | <p>Sets the default facility in the core.</p> <p>Some Opsware SAS processes use this name internally. It must be uppercase, less than 25 characters, and cannot contain spaces or special characters (although dashes and underscores are allowed).</p> <p>Source: Arbitrary.</p> <p>Example: HEADQUARTERS</p> |
| <p>Please enter the short name of the new facility you would like to define (Parameter: <code>slaveTruth.dcNm</code>)</p> | <p>Sets the default facility in the target core.</p> <p>Some Opsware SAS processes use this name internally. It must be less than 25 characters, and cannot contain spaces or special characters (although dashes and underscores are allowed).</p> <p>Source: Arbitrary.</p> <p>Example: NORTHSIDE</p> |

Table 5-4: Facility Prompts (continued)

| PROMPT | DESCRIPTION |
|--|---|
| Enter the default locale for users of the Opsware Command Center. (Parameter: <code>default_locale</code>) | Specifies the default locale (language, character sets, and date and time formats) for the Opsware SAS core. Source: In this release, the allowed values are <code>en</code> (English) and <code>ja</code> (Japanese). Example: <code>en</code> |
| Enter the facility long name. (Parameter: <code>truth.dcDispNm</code>) | Advanced: Sets the name that displays in the Opsware Command Center. It must be unique, less than 50 characters, and cannot include any special characters (<> & * \ ' ?). Source: Arbitrary. Example: Los Angeles Office |
| Please enter the long name for the facility that you are adding to the mesh. (Parameter: <code>slaveTruth.dcDispNm</code>) | Multimaster, Advanced: Sets the name of the target core that displays in the Opsware Command Center. It must be unique, less than 50 characters, and cannot include any special characters (<> & * \ ' ?). Source: Arbitrary. Example: Toronto Office |

Table 5-4: Facility Prompts (continued)

| PROMPT | DESCRIPTION |
|--|---|
| <p>Enter the facility ID (number only, less than 1000, with no leading zeros).</p> <p>(Parameter: <code>truth.dcId</code>)</p> | <p>Specifies the ID that uniquely identifies a facility.</p> <p>When you install a standalone core, you choose the facility ID during the installer interview.</p> <p>When you install a target core in a multimaster mesh, the facility ID is automatically generated when you add the facility in the Opsware Command Center. You specify this automatically-generated ID during the installer interview.</p> <p>Find the target facility ID by logging into the Opsware Command Center at the source facility. Select Opsware Facilities under Environment in the navigation panel and click the facilities' name.</p> <p>REQUIREMENT</p> <p>Opsware facility IDs must be less than 1000. Therefore, you must specify a number for the first facility that is well below 1000 so you can continue to add facilities to your multimaster mesh. If the Opsware Command Center automatically generates a number that is 1000 or higher, the installation will fail.</p> <p>Source: Arbitrary for the first facility; set by the Opsware SAS for subsequent facilities.</p> <p>Example: 100</p> |

Opsware SAS Feature Prompts

The following prompts are required to configure the OS Provisioning, Software Provisioning, Patch Management, and NAS Integration features in Opsware SAS.

The response to the prompt for the windows utilities directory depends on the steps you performed in “Patch Management Requirements” on page 57.

Table 5-5: Opsware SAS Feature Prompts

| PROMPT | DESCRIPTION |
|---|--|
| <p>Please enter the directory that contains Microsoft's qchain.exe, mbsacl.exe, mssecure.cab, wusscan.dll, mbsacl20.exe, WindowsUpdateAgent20-x86.exe and wsusscan.cab files</p> <p>(Parameter: windows_util_loc)</p> | <p>Specifies the directory to which you've copied the Microsoft utilities required for the Patch Management feature on Windows.</p> <p>Source: Arbitrary. (However, this directory must exist on the server where the Software Repository is installed.)</p> <p>Example: /home/win_util</p> |
| <p>Enter the OS Provisioning Boot Server IP or host name.</p> <p>(Parameter: bootagent.host)</p> | <p>Specifies the server on which you will install the OS Provisioning Boot Server component.</p> <p>You must provide a valid IP address or host name that can be resolved from the server on which you installed the OS Provisioning Boot Server and the Build Manager. Additionally, the host name must be resolvable by Opsware managed servers for OS provisioning.</p> |
| <p>Enter the host name or IP of the Build Manager.</p> <p>(Parameter: boot_server.buildmgr_host)</p> | <p>Specifies the server on which you will install the OS Provisioning Build Manager.</p> <p>You must provide a valid IP address or host name that can be resolved from the server on which you install the OS Provisioning Boot Server.</p> |
| <p>Enter the default network speed/ duplex setting for Solaris servers.</p> <p>(Parameter: boot_server.speed_duplex)</p> | <p>Sets the default network speed and duplex that will be used by Solaris servers booted from this boot server during Opsware OS provisioning. Valid responses are 100fdx, 100hdx, 10fdx, 10hdx, 100T4, and autoneg.</p> <p>Enter a value without spaces.</p> <p>Source: Arbitrary.</p> <p>Example: 100fdx</p> |

Table 5-5: Opware SAS Feature Prompts

| PROMPT | DESCRIPTION |
|---|---|
| <p>Enter the pathname of the Red Hat Linux media.</p> <p>(Parameter: <code>media_server.linux_media</code>)</p> | <p>Specifies the path to the Linux OS media on the server on which the Software Repository will be installed.</p> <p>Providing the path to the Linux OS media does not actually copy the media to this host.</p> <p>See the <i>Opware® SAS User's Guide</i> for the steps required to set up the media on the Media Server.</p> <p>Source: Arbitrary. (However, this directory must exist on the server where the Software Repository is installed.)</p> <p>Example: <code>/home/os_media/linux/</code></p> |
| <p>Enter the pathname of the Solaris media.</p> <p>(Parameter: <code>media_server.sunos_media</code>)</p> | <p>Specifies the path to the Sun Solaris OS media on the server on which the Software Repository will be installed.</p> <p>Providing the path to the Solaris OS media does not actually copy the media to this host.</p> <p>See the <i>Opware® SAS User's Guide</i> for the steps required to set up the media on the Media Server.</p> <p>Source: Arbitrary. (However, this directory must exist on the server where the Software Repository is installed.)</p> <p>Example: <code>/home/os_media/solaris/</code></p> |

Table 5-5: Opsware SAS Feature Prompts

| PROMPT | DESCRIPTION |
|--|--|
| <p>Enter the pathname of the Windows media.</p> <p>(Parameter: <code>media_server.windows_media</code>)</p> | <p>Specifies the path to the Microsoft Windows OS media on the server on which the Software Repository will be installed.</p> <p>The OS Provisioning feature exports Windows OS media to SMB clients through a Samba share.</p> <p>Providing the path to the Windows OS media does not actually copy the media to this host.</p> <p>See the <i>Opsware® SAS User's Guide</i> for the steps required to set up the media on the Media Server.</p> <p>Source: Arbitrary. (However, this directory must exist on the server where the Software Repository is installed.)</p> <p>Example: <code>/home/os_media/windows/</code></p> |
| <p>Enter the share name to use for the Windows media sharing server.</p> <p>(Parameter: <code>media_server.windows_share_name</code>)</p> | <p>Advanced: Sets the share name that you want Samba to use to export the Windows OS media.</p> <p>The share name is not case sensitive.</p> <p>Source: Arbitrary.</p> <p>Example: <code>WINMEDIA</code></p> |
| <p>Enter a password to write-protect the Windows media share. Import media prompts for this password each time it is run.</p> <p>(Parameter: <code>media_server.windows_share_password</code>)</p> | <p>Advanced: Sets the root user password, which enables write access to the Windows share. The Opsware Import Media Tool prompts for this password each time it is run.</p> <p>The password cannot contain spaces.</p> <p>Source: Arbitrary.</p> <p>Example: <code>x145_pwd03</code></p> |

Table 5-5: Opsware SAS Feature Prompts

| PROMPT | DESCRIPTION |
|---|--|
| <p>Please enter the root directory for the Package Repository.</p> <p>(Parameter: <code>word_root</code>)</p> | <p>Specifies the directory where packages are stored on the Software Repository for the Software Provisioning feature. Make sure this directory has sufficient free disk space. By default, packages are stored in the <code>/var/opt/opsware/word</code> directory on the Software Repository.</p> <p>Source: Arbitrary.</p> <p>Example: <code>/var/opt/opsware/word</code></p> |
| <p>Please enter the hostname or IP address of the NAS server. (Enter "none" if NAS is not installed.)</p> <p>(Parameter: <code>twist.nasdata.host</code>)</p> | <p>When your Opsware SAS core includes the NAS Integration feature, specifies the hostname or IP address of the server running the Network Automation System (NAS). If NAS has not been installed for your company, keep the default value, which is <code>none</code>, for this prompt.</p> <p>Enter a value without spaces.</p> <p>Source: Your network administrator or Opsware administrator who installed the Network Automation System.</p> <p>Example: <code>192.168.165.242</code></p> |

Opsware Gateway Prompts

These prompts are for the IP addresses and ports at which Opsware Gateways can be contacted by core components, Agents, or other Opsware Gateways. The port number must be less than 64001.

Table 5-6: Opsware Gateway Prompts

| PROMPT | DESCRIPTION |
|---|---|
| <p>Please enter the port on which the administrative interface for the core gateway will run.</p> <p>(Parameter: <code>cgw_admin_port</code>)</p> | <p>Advanced: Specifies the port of the Opsware Gateway's administrative interface, which allows you to view the configuration and monitor traffic flow.</p> <p>Source: Arbitrary.</p> <p>Example: 8085</p> |
| <p>Please enter the IP address of the core Opsware Gateway.</p> <p>(Parameter: <code>cgw_address</code>)</p> | <p>Specifies the IP address of the Opsware Gateway in the core at which other core components and Gateways can contact the core. In an Opsware Satellite installation, this IP address points to the core Gateway contacted by the Satellite.</p> <p>Source: Arbitrary.</p> <p>Example: 192.168.165.242</p> |
| <p>Please enter the port on which core components can contact this gateway to request tunneled connections.</p> <p>(Parameter: <code>cgw_proxy_port</code>)</p> | <p>Advanced: Specifies the port of the Opsware Gateway in the core at which components in the same core can request connections to other components.</p> <p>Source: Arbitrary.</p> <p>Example: 3002</p> |
| <p>Please enter the port on which Agents can contact the gateway to request connection to core components.</p> <p>(Parameter: <code>agw_proxy_port</code>)</p> | <p>Specifies the port of the Opsware Gateway in the core at which Opsware Agents can request connections to core components.</p> <p>Source: Arbitrary.</p> <p>Example: 3001</p> |

Table 5-6: Opware Gateway Prompts (continued)

| PROMPT | DESCRIPTION |
|---|--|
| Please enter the port on which this gateway will listen for connections from other gateways. (Parameter: <code>cgw_tunnel_listener_port</code>) | Specifies the port at which this Opware Gateway will listen for connections from other Opware Gateways. Source: Arbitrary. Example: 2001 |

Opware Global File System Prompts

The following prompts are for specifying IP addresses and directories for the Opware Global File System.

Table 5-7: Opware Global File System Prompts

| PROMPT | DESCRIPTION |
|--|---|
| Please enter the IP or host name of the nfs server for the Opware Global File System user home and tmp directories. (Parameter: <code>ogfs.store.host</code>) | Advanced: Specifies the server from which the storage for the home and tmp directories for the Opware Global File System will be mounted. Source: Arbitrary. Example: 192.168.198.92 |
| Please enter the absolute path on the nfs server for the Opware Global File System user home and tmp directories. (Parameter: <code>ogfs.store.path</code>) | Advanced: Specifies the directory for the storage of the home and tmp directories of the Opware Global File System. Source: Arbitrary. Example: <code>/cust/ogfs/store</code> |
| Please enter the IP or host name of the nfs server for the Opware Global File System where the audit streams will be stored. (Parameter: <code>ogfs.audit.host</code>) | Advanced: Specifies the IP address of the server where storage for audit streams for the Opware Global File System will be mounted. Source: Arbitrary. Example: 192.168.165.242 |

Table 5-7: Opware Global File System Prompts (continued)

| PROMPT | DESCRIPTION |
|---|--|
| <p>Please enter the absolute path on the nfs server for the Opware Global File System where the audit streams will be stored.</p> <p>(Parameter: <code>ogfs.audit.path</code>)</p> | <p>Advanced: Specifies the path for the storage of the audit streams for the Opware Global File System.</p> <p>Source: Arbitrary.</p> <p>Example: <code>/cust/ogfs/audit</code></p> |
| <p>Please enter comma-separated list of IP address(es) for the devices where the Opware Global File System (OGFS) is going to be installed in this facility (ip,ip...).</p> <p>(Parameter: <code>hub.ip</code>)</p> | <p>Specifies one or more IP addresses of the servers on which to install the Opware Global File System.</p> <p>Multiple entries are separated by commas.</p> <p>Source: Arbitrary.</p> <p>Example: <code>192.168.198.92</code></p> |
| <p>Please enter the pathname of where you wish the local cache of snapshots and audits to be. This will require a large amount of disk space (4G by default).</p> <p>(Parameter: <code>spoke.cachedir</code>)</p> | <p>Specifies the directory where the Global File System service stores snapshots and audits for quick access. By default, the Audit and Remediation features stores snapshots and audits in the directory <code>/var/opt/opsware/compliancecache</code>.</p> <p>This cache area is set up to use 4 GB of disk space.</p> <p>Source: Arbitrary.</p> <p>Example: <code>/var/opt/opsware/compliancecache</code></p> |

Uninstallation Prompts

The prompts in the following table appear when you are uninstalling an Opware core.

Table 5-8: Uninstallation Prompts

| PROMPT | DESCRIPTION |
|---|--|
| <p>Do you need to preserve any of the data in this database?</p> <p>(Parameter: <code>truth.uninstall.needdata</code>)</p> | <p>Because uninstalling the Model Repository permanently deletes all data in the database, the uninstallation process stops if you answer yes to this parameter, so you have the opportunity to back up the data you would like to preserve. The Opware Installer does not preserve any data.</p> <p>Example: <code>y</code></p> |
| <p>Are you sure you want to remove all data and schema from this database?</p> <p>(Parameter: <code>truth.uninstall.aresure</code>)</p> | <p>Because uninstalling the Model Repository permanently deletes all data in the database, the uninstallation process stops if you answer no to this parameter.</p> |
| <p>Would you like to preserve the database of cryptographic material?</p> <p>(Parameter: <code>save_crypto</code>)</p> | <p>If you answer yes, the database of cryptographic material is saved. Otherwise, it is deleted when the uninstallation finishes.</p> <p>Example: <code>y</code></p> |
| <p>Are you absolutely sure you want to remove all packages in the repository?</p> <p>(Parameter: <code>word.remove_files</code>)</p> | <p>If you answer yes, the packages, logs, and cryptographic material for the Software Repository are removed.</p> <p>Example: <code>y</code></p> |

Opware Installer

This section discusses the following topics:

- Installation Media for the Opware Installer
- Opware Installer Command Line Syntax
- Installer Interview

- Opsware Installer Logs

Installation Media for the Opsware Installer

Opsware SAS is available on and installable from the following DVD set, which contains the scripts for installing, uninstalling, and upgrading components.

- **Product Software:** Contains all packages and scripts necessary to install an Opsware SAS core, including Oracle RDMBS.
- **Agent and Utilities:** Contains packages, (such as the OS Provisioning Boot Agent, Opsware Agents for each operating system, etc.) that need to be uploaded to the Software Repository once the Opsware SAS core has been installed.
- **Satellite Base:** Contains packages and scripts necessary to install the Opsware Gateway and the Software Repository Cache in the Satellite.
- **Satellite Base Including OS Provisioning:** Contains packages and scripts to install Software Repository Caches, Opsware Gateways, and OS Provisioning components in the Satellite.

For the script names, see “Opsware Installer Command Line Syntax” on page 97.

Copying the DVD to a Local Disk

Opsware Inc. recommends that you copy the contents of the Opsware SAS DVDs to a local disk or to a network share and run the Opsware Installer from that location. When you copy the contents of an Opsware SAS DVD to a local disk or the network, you must create a directory structure that duplicates the structure of the DVD, for example:

```
/opsware_system
```



The path of the directory where you copy the contents of the DVD cannot have spaces.

When you run the Opsware Installer from the common parent directory, `/opsware_system`, the Opsware Installer switches automatically to the directory it needs to complete the part of the installation process that it is currently performing.

Opsware Installer Command Line Syntax

The Opsware Installer is run by using one of the following three scripts:

- `install_opsware.sh` – installs a component

- `upgrade_opsware.sh` – upgrades a component
- `uninstall_opsware.sh` – uninstalls a component

All three of these scripts run with the same command line options, as the following table shows.

Table 5-9: Opware Installer Command Line Options

| OPTION | DESCRIPTION |
|--|--|
| -h | <p>Display the Opware Installer help for the command line options.</p> <p>To display help during the interview, press <code>ctrl-I</code>.</p> |
| <p>--resp_file=<i>file</i></p> <p>(-r <i>file</i>)</p> | <p>Install an Opware component, using the values in the specified response file.</p> <p>The installer prompts for the component to install and then runs an interview that only prompts for data missing in the response file. If the response file is incomplete, the installer prompts for the missing information.</p> <p>The installer keeps an inventory of the components that are installed on a given server.</p> |
| --interview | <p>Conduct the installation interview to obtain values for component parameters. At the end of the interview, the installer saves the values in the response file.</p> <p>Usually, you specify this option when you run the Opware Installer on the host where the Model Repository has been or will be installed. You also specify this option when you have a complete response file but need to run the installer in a different mode, such as converting a standalone core to multimaster.</p> <p>If you specify both the <code>--interview</code> and <code>--resp_file</code> options, the installer runs the interview, using the values in the response file as the defaults.</p> <p>If you specify no command line options, the installer runs as if you specified the <code>--interview</code> option.</p> |
| --verbose | Run the installer in verbose mode. |

Installer Interview

The interview prompts you for the mode, either simple or advanced. In the simple mode, the interview does not prompt for parameters that are rarely modified. (Such parameters include the various Oracle passwords used internally by the Opsware components.) If you use the simple mode, the installer will use default values for these parameters. In the advanced mode, the installer prompts for all parameters that are relevant to the type of installation.

The installer validates responses to the interview prompts as you enter them; you are asked to re-enter a value until the installer is able to validate the answer. Some parameters are also revalidated during the actual installation of components. If a response to a prompt cannot be validated at installation, the installer runs a mini-interview.

At any time during the interview, you can press `ctrl-I` to display help for the current prompt.

After all parameters have values, the installer asks if you want to finish the interview. If you want to go back and review or change your answers, press `n`. If you press `y`, the installer prompts for the name of the response file in which it will save your answers. (The directory containing the response file must exist.) After saving the file, the installer asks if you'd like to continue the installation using the data from the response file. If you press `y`, the installer displays the Opsware components to install. If you press `n`, the installer exits.

When you install a core on multiple servers, you should copy the response file to the other servers so that the installations of subsequent components can use the data in the response file.

Opsware Installer Logs

Each time you run the Opsware Installer, it generates the following log file:

```
/var/log/opsware/install_opsware/install_opsware.timestamp.log
```

If you specify the `--verbose` option, the following log file is created:

```
/var/log/opsware/install_opsware/install_opsware.timestamp_
verbose.log
```

Some components have supplementary logs that contain additional details about the installation of those components.

The installation of the Model Repository creates the following log files:

```
/var/log/opsware/install_opsware/truth/truth_install_number.log
```

```
/var/log/opware/install_opware/truth/truth_install_number_
verbose.log
```

Chapter 6: Opware Standalone Installation

IN THIS CHAPTER

This section discusses the following topics:

- Overview of the Standalone Installation
- Prerequisites for Installing a Standalone Core
- Installing a Standalone Core
- Opware Command Center Web Client
- Logging into the Opware Command Center

Overview of the Standalone Installation

A standalone core manages servers in a single facility. The following steps provide an overview of the standalone installation process. For detailed instructions, see “Prerequisites for Installing a Standalone Core” on page 102.

In an Opware SAS core, the Opware Model Repository uses an Oracle database. This chapter provides the instructions for installing an Opware SAS standalone core with Oracle 10g by using the Opware Installer.

For information about installing an Opware SAS core by using an existing Oracle database, contact your Opware support representative.

- 1** Obtain the Opware SAS installation DVDs.
- 2** Run the Opware Installer (`install_opware.sh` script) in interview mode. The interviewer prompts you for information about your environment and saves the information in a response file.
- 3** Run the Opware Installer and select the Opware components to install. In this step, the Installer creates the Opware directories and files on a server. For a single-server installation, you only need to run the Installer once. For a multiple servers, you log on

to each server and run the Installer, specifying the components to install. You must install the Opware core components in the order displayed by the Opware Installer (see step 14 on page 104).

Prerequisites for Installing a Standalone Core

Before you install a standalone core, you must perform the following tasks:

- Plan your Opware System deployment. When planning for a core, you must decide whether you want to install the core components on a single server or on multiple servers. See Chapter 1, “Opware SAS Architecture” and “Opware Core Scalability for Performance” on page 43.
- Perform the pre-installation administration tasks such as configuring the network. See Chapter 3, “Pre-Installation Requirements.”
- Gather information in preparation for the Opware Installer interview. This information includes the name and ID of the facility for the core. See Chapter 5, “Prerequisite Information for the Installer Interview.”

Installing a Standalone Core

This section contains step-by-step instructions for running the Opware Installer (`install_opware.sh` script).

- 1** Obtain the Opware Server Automation System (SAS) installation media.
See “Installation Media for the Opware Installer” on page 97, including the recommendation, “Copying the DVD to a Local Disk.”
- 2** On each server where you will install the new Opware core, mount the Product Software DVD or NFS-mount the directory that contains a copy of the DVD contents.
The Opware Installer must have read/write root access to the directories where it installs Opware components, even NFS-mounted network appliances.
- 3** On the server where you want to install the Opware Model Repository, in a terminal window, log in as root.
- 4** Change to the root directory:
`cd /`

- 5** Run the Opware Installer in interview mode by invoking it with no command-line options:

```
/opware_system/opware_installer/install_opware.sh
```

You must specify the full path to the script. The directory path shown in this step indicates that you copied the Opware SAS Product Software DVD to a local disk or network share by using the required directory structure.

The Opware Installer displays the following options:

```
Welcome to the Opware Installer. Please select one of the
following installation options:
```

```
1 - Standalone Installation: Standalone Opware Core
2 - Multimaster Installation: First Core (convert from
standalone)
3 - Multimaster Installation: Define New Facility; Export
Model Repository
4 - Multimaster Installation: Additional Core
```

- 6** At the installation options prompt, select the following option:

```
1 - Standalone Installation: Standalone Opware Core
```

- 7** At the interview mode prompt, select one of the following options:

```
1 - Simple Interview Mode
2 - Advanced Interview Mode
```

Option 1 is for using default values for many of the configuration parameters. Option 2 is for specifying all configuration parameters during the interview.

- 8** At the database configuration option prompt, select the following option:

```
1 - Install Oracle with Opware
```

For information about installing an Opware SAS core by using option 2 (“Use Existing Oracle Database”), contact your Opware support representative. When you use an existing Oracle database, you must configure the Oracle database instance correctly to work with the Opware SAS core.

- 9** Respond to the interview prompts.

The installer displays default values in square brackets [].

See “Required Information for Running the Installer Interview” on page 75.

When you run the interview, the paths for the OS provisioning media must already exist on the server where you will install the OS Provisioning Media Server component.

10 Decide if you want to finish the interview.

When you enter all of the required information, the Opware Installer displays this message:

```
All parameters have values. Do you wish to finish the
interview (y/n):
```

If you are satisfied with your answers, press y.

If you want to review or change your answers, press n. The installer displays the prompts again, showing in brackets [] the values that you previously entered.

If you are satisfied with your answers, press y.

11 Create the response file.

When you are finished with the interview, the installer prompts you for the name of the response file:

```
Name of response file to write
[/usr/tmp/oiresponse.stand_single]
```

The response file is a text file that contains the answers you entered during the interview. You can enter the full path and name of the response file or accept the default. In either case, write down the name of the response file. Note that the default file name corresponds to the type of installation.

12 The Opware Installer prompts you to indicate whether you want to continue the installation by using the response file:

```
Would you like to continue the installation using this
response file? (y/n):
```

If you are satisfied with the responses you entered in the interview and you are ready to install the Model Repository now, enter y to continue. If you do not want to install the Model Repository now, enter n.

13 If you entered y in the previous step, skip this step. If you entered n in the previous step, invoke the Opware Installer with the -r option to specify the response file created by the interview:

```
/opware_system/opware_installer/install_opware.sh -r
<full_path_to_response_file>
```

14 At the components prompt, select one or more components to install:

```
Welcome to the Opware Installer.
```


Please select the components to install.

- 1 () Oracle RDBMS
- 2 () Model Repository (truth)
- 3 () Data Access Engine (spin)
- 4 () Command Engine (way)
- 5 () Software Repository (word)
- 6 () Opware Global Filesystem Server (OGFS)
- 7 () Opware Command Center (OCC)
- 8 () OS Provisioning Media Server
- 9 () OS Provisioning Build Manager
- 10 () Opware Gateway
- 11 () OS Provisioning Boot Server

Enter a component number to toggle ('a' for all, 'n' for none).

When ready, press 'c' to continue, or 'q' to quit.

Selection:

You must install the components in the order they are listed. For example, you must install the Model Repository before the Data Access Engine.

If you are installing all of the components on a single server, then you may enter a for all. If you do not select a, then you must run the Opware Installer again (specifying the response file) and select the remaining components. (If you are installing the components on multiple servers, see the next step.)

For some of the components, such as the OS Provisioning Build Manager, the Installer interview prompts you for the IP address or host name. Be sure to install these components on the host that you indicated during the interview.

15 If you are installing the components on multiple servers, follow the instructions in this step. (If you are installing the components on a single server, skip this step.)

- Copy the response file generated by the installer interview to all other servers in this core.
- After you install the Model Repository, copy the Oracle `tnsnames.ora` file from the server with the Model Repository to the other Opware core servers. The directory path for the file must be the same on all core servers. (By default, `tnsnames.ora` is in the `/var/opt/oracle` directory.)
- On each server in this core, run the Opware Installer with the `-r` option, as shown in step 13. Select and install the remaining components from the menu shown in step 14.

- For the Model Repository, the installer asks if you want to generate cryptographic material, enter `y`. Copy the database of cryptographic material and the Unix Tar file Gzipped from the following directory to every Opsware core server:

```
/var/opt/opsware/crypto/cadb/realms/opsware-crypto.db.e
```

```
/var/opt/opsware/crypto/cadb/realms/opsware-crypto.tgz.e
```

The database of cryptographic material and the Tar file Gzipped must be copied to the same directory and file names on every Opsware core server. The directory and database need to be readable by the root user.

- If the Model Repository or Boot Server exist on a server with no other Opsware components installed on it, you must install an Opsware Agent on that server. See the *Opsware® SAS User's Guide: Server Automation* for instructions.

16 (Optional) If you are distributing the core components across multiple servers, you can install additional instances of the following components:

- Data Access Engine

If you install more than one Data Access Engine, then you must perform the procedure described in “Reassigning the Data Access Engine to a Secondary Role” in the *Opsware® SAS Administration Guide*.

- OS Provisioning Media Server
- Opsware Command Center
- Opsware Global File System Server (OGFS)

To install multiple instances of the OGFS when you install an Opsware core, during the Opsware Installer interview, specify the IP addresses of the servers on which you plan to install the OGFS.

To install additional instances of the OGFS to an existing core, you must perform manual steps. See Chapter 7, “Adding Instances of the Opsware Global File System Server (OGFS) to a Core” on page 131 of this guide for more information.

17 On the server where you installed the Software Repository, mount the Agent and Utilities DVD or NFS-mount the directory that contains a copy of the DVD contents.

The Opsware Installer must have read/write root access to the directories where it installs Opsware components, even NFS-mounted network appliances.

18 In a terminal window, log in as root and change to the root directory:

```
cd /
```

- 19** Invoke the Opware Installer with the `-r` (response file) option. For example:

```
/opware_system/opware_installer/install_opware.sh -r  
/usr/tmp/oiresponse.stand_single
```

You must specify the full path to the script. The directory path in the preceding command indicates that you copied the Opware SAS Agent and Utilities DVD to a local disk or network share using the required directory structure.

You should run the Opware Installer with the response file that you created when you installed the standalone core.

The Opware Installer displays the following options:

```
Welcome to the Opware Installer. Please select the  
components to install:
```

```
1 ( ) Software Repository - Content
```

- 20** At the install prompt, select option 1:

```
1 ( ) Software Repository - Content
```

- 21** Follow the instructions in the following section, “Opware Command Center Web Client” on page 107.

- 22** Follow the instructions in “Post-Installation Tasks” on page 111.

Opware Command Center Web Client

After you install an Opware SAS core, you should be able to log into the Opware Command Center web client.

To run the Opware Command Center, 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.

Logging into the Opware Command Center

- 1** In a web browser, enter the following URL:

```
https://<ip-address-occ>
```

The <ip-address-occ> is the IP address of the server on which you installed the Opware Command Center component.

- 2** Follow the browser's instructions for installing the security certificate.
- 3** When the Opware Command Center prompts you for the user name and password, enter `admin` for the user name. For the password, enter the value for the `cast.admin_pwd`, which you specified during the Installer interview.
- 4** Create a new user by using the Users & Groups page under Administration. For the Group Membership, select Opware System Administrators.

See the *Opware® SAS Configuration Guide* for information about creating Opware users.
- 5** Log into the Opware Command Center as the user you created in the previous step. Run the Opware System Diagnosis by clicking System Diagnosis under Administration in the navigation panel.

See the *Opware® SAS Administration Guide* for information about the procedures for running the system diagnosis tool.
- 6** Log into the Opware Command Center as the `admin` user again. Create a new user and for the Group Membership, select Advanced Users.
- 7** Log into the Opware Command Center as the user you created in the previous step. Exercise the different Opware System functions by clicking the links in the left navigation panel and by opening the wizards on the home page.

Chapter 7: Post-Installation Tasks

IN THIS CHAPTER

This section discusses the following topics:

- Setup for Opsware Discovery and Deployment
- Setting Up NAS Integration
- DHCP Configuration for OS Provisioning
- Additional Network Requirements for OS Provisioning
- Patch Management on Windows NT 4.0 and Windows 2000

Setup for Opsware Discovery and Deployment

With the Opsware Discovery and Deployment (ODAD) feature you can use the SAS Client to install Opsware Agents on servers.

Enabling the ODAD Feature for Unix Servers

Enabling the ODAD feature for Unix servers does not require that you perform additional set up steps. When you run the Opsware Installer, it automatically installs all required software to use the ODAD feature with Unix servers.

However, before you use the ODAD feature to open remote terminal sessions on unmanaged Unix servers, verify that the following requirement has been met.

On the server with the Agent Gateway, the `telnet`, `rlogin`, and `ssh` clients must reside in either the `/bin`, `/usr/bin`, or `/usr/local/bin` directory. If the client resides in a different directory, create a symbolic link in `/usr/local/bin` to the actual location of the client.

Enabling the ODAD Feature for Windows Servers

Before you can use the ODAD feature to deploy Opsware Agents to Windows servers, you need to install additional software on a Windows server and configure the Opsware Gateway as described in “Installing the Windows Agent Deployment Helper” on page 112.

Installing the Windows Agent Deployment Helper

Before using the ODAD feature to install Agents on Windows servers, you must install the Windows Agent Deployment Helper package.



You need to install only one Windows Agent Deployment Helper for each Opware core. You cannot install a Windows Agent Deployment Helper in an Opware Satellite.

To install the Windows Agent Deployment Helper, perform the following steps:

- 1** Obtain a Windows server on which you can install the Windows Agent Deployment Helper. This server must be running a 32-bit version of Windows 2000, Windows 2003, or Windows XP. (Windows 64-bit operating systems are not supported.)

On this Windows server, install an Opware Agent with the command-line utility. See the *Opware® SAS User's Guide* for instructions on how to install an Opware Agent.
- 2** Log into the SAS Client. See the *Opware® SAS User's Guide: Server Automation* for information.
- 3** From the Navigation pane, select **Devices** ► **All Managed Servers**.
- 4** From the Content pane, select the Windows server on which you installed the Opware Agent.
- 5** From the Action menu, select **Attach** ► **Attach Software Policy**. The Attach Software Policy window appears.
- 6** From the list of software policies, select Windows Agent Deployment Helper. (By default, the Remediate Servers Immediately option is selected. Do not deselect this option.)
- 7** Click **Attach**. The Remediate window appears.
- 8** Complete the tasks to remediate the server with the Windows Agent Deployment Helper policy. See the *Opware® SAS User's Guide: Application Automation* for the steps to remediate a server with a software policy.
- 9** Restart any running OCC Clients.

The restart is needed because the OCC Client caches information about the Windows Agent Deployment Helper.

- 10** Log in as `root` to the server with the core Gateway. With a text editor, open the following file:

```
/etc/opt/opsware/opswgw-cgw0-<facility>/opswgw.properties
```

- 11** Locate the following line:

```
#opswgw.IngressMap=${NETBIOSHELPERIP}:NETBIOS
```

- 12** Uncomment the line, and replace `${NETBIOSHELPERIP}` with the IP address of the server where you installed the Windows Agent Deployment Helper. For example:

```
opswgw.IngressMap=192.168.165.242:NETBIOS
```

- 13** Restart the core Gateway with the following command:

```
/etc/init.d/opsware-sas restart opswgw-cgw0
```

Details: Agent Deployment Helper Setup for Disabled Administrator Account

When the Windows Administrator account is disabled on a Windows server, you must perform the following additional setup steps for installing the Agent Deployment Helper.

- 1** Log on as `root` to a server running an Opsware SAS component.
- 2** Change directories to the following directory:

```
cd /opt/opsware/oi_util/bin/
```

- 3** Enter the following command to run the `shared_script_util.sh` script


```
./shared_script_util.sh modify adt_deploy_agents.bat -U  
ACCOUNT_NAME -p agentDeployment.deployAgent -e -c "Change  
user name"
```

Where `ACCOUNT_NAME` is the name of the account you want the script to run as.

- 4 (Optional)** Enter the following command to review the current script settings:

```
./shared_script_util.sh showpolicy adt_deploy_agents.bat
```

You will see the following output, except that the `USER` line should contain the name of the account you just set.

```
PTY 0  
USER Administrator  
EXEMPT  
PERM agentDeployment.deployAgent
```

Setting Up NAS Integration

To set up the NAS Integration feature, you must change configuration settings in NAS and in SAS, run diagnostics for NAS topology data, and set up user permissions.



To set up NAS Integration, you must have Opsware Network Automation System (NAS) 6.1 installed.

Optionally, you can reset the NAS host name if the SAS Client is not communicating (cannot find) the NAS server as it is currently defined.



When setting up the NAS Integration feature, the Opsware NAS core and the Opsware SAS core can share an Opsware Gateway instance only under the following condition. You can add NAS support to an existing SAS Gateway so that it preserves SAS capability. However, adding SAS support to an existing NAS Gateway is *not* supported in this release.

Configuration for the NAS Integration Feature

To set up the NAS Integration feature, you must change the following two configuration settings, one in NAS and then one in SAS:

- A configuration setting in NAS (which you must make *first*)
- A configuration setting in a SAS .conf file (*after* you made the NAS change)

NAS Configuration

To change the configuration setting in NAS, perform the following steps:

- 1** Log in to Opsware NAS.

- 2 Select **Admin** ► **Administrative Settings** ► **User Authentication** to display the Administrative Settings – User Authentication page.

Figure 7-2: External Authentication Type in NAS

Administrative Settings - User Authentication Add to Favorites Help

Notes:
Leaving this page or clicking any hyperlinks without clicking the Save button will result in the loss of any unsaved changes to the admin settings.

Configuration Mgmt | Device Access | Server | Workflow | User Interface | Telnet/SSH | Reporting | **User Authentication** | Server Monitoring

Save

User Password Security

Minimum User Password Length: (in characters)

User Password Must Contain Upper and Lower Case: Requires users to choose passwords which contain both lower-case and upper-case alphabetic characters.

Additional User Password Restriction:

- No additional restrictions
- Must contain at least one non-alphabetic digit or special character
- Must contain both at least one digit and at least one special character

Maximum Consecutive Login Failures: Maximum number of allowed consecutive user authentication failures, after which the user will be disabled. A value of 0 (zero) indicates that this check should be skipped. Note that this setting applies only to built-in user authentication and not to external authentication methods.

External Authentication Type

External Authentication Type:

- None (Local Auth)
- Opsware Server Automation System
- TACACS+
- RADIUS
- SecurID
- Active Directory

 (After saving the settings, go to Active Directory Setup page for more options)

Choose the type of external authentication you would like to use. If you choose TACACS+, RADIUS or Opsware, it can be configured in the section below. SecurID has no additional external authentication options.

- 3 In the External Authentication Type section, select Opsware Server Automation System.

Figure 7-3: Opsware Server Automation System Authentication

| Opsware Server Automation System Authentication | |
|---|---|
| Twist Server | <input type="text" value="twist.c43.dev.opsware.com"/> Web Services Data Access Engine host name or IP address |
| Twist Port Number | <input type="text" value="1032"/> Web Services Data Access Engine listening port (typically 1026) |
| Twist Username | <input type="text" value="detuser"/> Web Services Data Access Engine Username for finding connected servers. |
| Twist Password | <input type="password" value="....."/> Web Services Data Access Engine Password for finding connected servers. |
| OCC Server | <input type="text" value="occ.c43.dev.opsware.com"/> Opsware Command Center host name for linking to connected servers. |
| Default User Group | <input type="text" value="Limited Access User"/> User Group for new Server Automation System user |

- 4 Complete all fields in the Opsware Server Automation System Authentication section. NAS uses the Twist Username and Twist Password when it gathers layer 2 data. NAS looks for the server interface information by MAC address, using that user's permissions. The user must have read access to server information.

- 5 Click **Save** to save your configuration change.

See the *Opware® NAS User's Guide*.

SAS Configuration

If the NAS server name was not entered during SAS installation, you must add the `twist.nasdata.host=<hostname>` setting in the `twist.conf` file in `/etc/opt/opware/twist/twist.conf`. See the *Opware® SAS Planning and Installation Guide*.



After you make these configuration changes, you must restart NAS and the Twist.

Topology Data

To continue setting up the NAS Integration feature, you must also run the NAS Topology Data Gathering and NAS Duplex Data Gathering diagnostics in NAS. See the *Opware® SAS User's Guide: Server Automation* and the *Opware® NAS User's Guide*.

User Permissions for the NAS Integration Feature

Access permissions for the NAS Integration feature are based on two separate databases: a NAS database and a SAS database. NAS uses its own database for authorization. SAS uses a different security mechanism for authorization. However, all authentication (for both NAS and SAS) is processed by SAS.

When NAS is configured to use SAS authentication, it tries to authenticate against SAS first. If NAS fails to authenticate against SAS, it falls back to the NAS database. If there is an account in the NAS database, the fallback is only allowed if that user is configured to allow fallback authentication. See the *Opware® NAS User's Guide*.

When a new user is authenticated through SAS, an account is created in NAS and placed in the Default User Group that was specified when SAS authentication was enabled in the Administrative Settings in NAS. This user group is configurable – which user group is specified and what permissions the system administrator has assigned to that group controls the actions that will be allowed in NAS.



You must have a set of permissions to view servers and network devices, and make configuration changes. To obtain these permissions, contact your Opsware administrator. See the *Opsware® SAS Administration Guide*.

DHCP Configuration for OS Provisioning

The Dynamic Host Configuration Protocol (DHCP) specifies how to assign dynamic IP addresses to servers on a network. Opsware OS Provisioning uses DHCP to allow network booting and configuration of unprovisioned servers in the Server Pool. DHCP is also used to configure networking on newly provisioned servers that have not been assigned a static network configuration.

For OS provisioning, you may use either the DHCP server included Opsware SAS, an existing ISC DHCP server, or the MS Windows DHCP server. The instructions for configuring these various DHCP servers are in the following sections:

- Configuring the Opsware DHCP Server for OS Provisioning
- Configuring an Existing ISC DHCP Server for OS Provisioning
- Configuring the MS Windows DHCP Server for OS Provisioning
- Configuring the Opsware and MS Windows DHCP Servers for OS Provisioning

DHCP Software included with the Opsware Boot Server

When you install the Opsware Boot Server, the Opsware Installer also installs the following items:

- **dhcpcd**: An Internet Software Consortium DHCP server (ISC dhcpcd).
- **dhcpcd.conf**: A default configuration file, read by the `dhcpcd` server.
- **dhcpcdtool**: The Opsware DHCP Network Configuration Tool, writes to the `dhcpcd.conf` file.

Opsware DHCP Server (*dhcpcd*)

The DHCP server provides service to two types of networks:

- **Local networks**: Networks that are attached directly to the network interfaces of the host running the DHCP server. No special network configuration is needed to support local networks.

- **Remote networks:** Networks that are not directly attached to the DHCP server host. A router sits between the DHCP server host and the remote networks. For remote networks, a DHCP proxy (sometimes called IP helper) must be configured on each remote network to relay DHCP packets to the DHCP server host.

A DHCP proxy is not provided with Opware SAS and instructions for setting one up are beyond the scope of this document. DHCP proxy functionality is often included in modern routers. Check with your network administrator or router vendor.

Log messages that the DHCP server produces are sent to the standard Unix syslog process with the daemon facility. Consult your vendor documentation on how to configure and view syslog messages.

See “Starting and Stopping the Opware DHCP Server” on page 122.

Opware `dhcpd.conf` File

The `dhcpd.conf` file provides the necessary parameters to support network booting of Sun hardware (a DHCP-capable PROM is required) and x86 hardware (a PXE-compatible system is required).



For x86 hardware that does not support PXE, the server can be booted from a floppy (Windows) or CD (Linux). When a boot floppy or CD is used, the DHCP server still provides network configuration information to the host.

The DHCP configuration file is `/etc/opt/opware/dhcpd/dhcpd.conf`. In most cases, you will modify this file by running the DHCP Network Configuration Tool. For some advanced configurations (as noted in the following section), you may need to modify the file with a text editor. Documentation on the DHCP configuration file is available at the ISC web site www.isc.org.

The DHCP leases file is `/var/opt/opware/dhcpd/dhcpd.leases`. Normally, this file should not need editing.

Opware DHCP Network Configuration Tool (`dhcpdtool`)

The DHCP Network Configuration Tool is a menu-driven, terminal-based utility that enables you to customize the `dhcpd.conf` file for common local and remote network configurations. The tool prompts you for network information needed to configure DHCP

for each OS provisioning network. Using the DHCP Network Configuration Tool simplifies configuration of the DHCP server and ensures that the DHCP configuration contains the options that are needed for the OS Provisioning feature to function properly.

If you need to configure the network for Opware OS Provisioning to support less common configurations, you must modify the `dhcpd.conf` file with a text editor. Less common configurations include dual-interfaces with split-horizon DNS requirements, private build networks, and static NAT. Contact Opware Support for more assistance.

Additionally, in some environments, multiple IP networks (layer 3) are layered on top of a single VLAN (layer 2). While this configuration is supported by the ISC DHCP server, generally such a topology requires careful consideration to work properly with DHCP. Therefore, the DHCP Network Configuration Tool can only configure a single IP network per VLAN.

The man pages for the DHCP Network Configuration Tool are installed in `/opt/opware/dhcpd/man` on the Boot Server. They are also available at the Opware Support web site.

Required Information for the Opware DHCP Network Configuration Tool

Before you use the DHCP Network Configuration Tool to configure an OS provisioning network, you need the following information:

- The range of IP addresses that are assigned dynamically by the DHCP server. For example, 192.168.0.11, 192.168.0.20 might be used to configure a pool of 10 addresses. **Important:** Each of these IP addresses must resolve to a host name on the DNS server.
- The IP addresses of one or more DNS servers. The servers given must be able to resolve the standard required Opware DNS entries. The DNS servers do not need to be on the same network that is being configured.
- A default DNS domain. This domain must include the standard, required Opware DNS entries. For example, if the default DNS domain is `example.org`, then there must be an entry `spin.example.org` that can be resolved by the DNS servers.

If you are going to configure a remote network with the DHCP Network Configuration Tool, you will also need to provide the following information:

- The network address and size (netmask or bits). For example, 192.168.0.0/255.255.255.0 or 192.168.0.0/24. Both specify a network range of 192.168.0.0 - 192.168.0.255.

- The network gateway or default router, for example, 192.168.0.1.

Configuring the Opware DHCP Server for OS Provisioning

The DHCP Network Configuration Tool is installed with the Opware Boot Server. Perform the following steps to configure networks for OS provisioning:

1 Log in as root to the server running the Opware Boot Server.

2 Make a backup copy of the configuration file:

```
cd /etc/opt/opware/dhcpd
cp dhcpd.conf dhcpd.conf.orig
```

3 Run the DHCP Network Configuration Tool:

```
/opt/opware/dhcpd/sbin/dhcpdtool
```

The DHCP Network Configuration Tool main menu appears, as follows:

Example: DHCP Network Configuration Tool Main Menu

```
Opware DHCP Network Configuration Tool
```

```
a)dd a new network.
e)xit.
```

```
Choice [a, e]:
```

4 To add a new network, enter a at the preceding prompt.

The menu to add local or remote networks appears, as follows.

Example: Menu to Add Local or Remote Networks

```
Opware DHCP Network Configuration Tool
```

```
You may view/edit/delete one of the currently configured
network(s):
```

```
1) 192.168.164.0/28
2) 192.168.165.128/28
```

```
Or
```

```
a)dd a new network.
e)xit.
```


Choice [1..2, a, e]: a:

- 5** To configure the DHCP service on the local network, enter 1 at the preceding prompt. Local networks are detected automatically and displayed.

Or

To add a remote network, enter r at the preceding prompt.

- 6** If you are adding a local network, you need to enter the IP addresses or host names of the DHCP range and the DNS servers. In the example that follows, note that the IP addresses are separated by a comma and a space.

Example: Local Network Configuration

Opsware DHCP Network Configuration Tool

Editing DHCP information for 192.168.8.0/23 (255.255.254.0)

All values which prompt for an address accept either a IP or a hostname.

Enter the DHCP Range (start address, stop address)

: 192.168.8.20, 192.168.8.29

Enter the DNS server(s) (comma separated)

: 192.168.2.25, 192.168.2.28

Enter the DNS domain: opsware.com

- 7** If you are adding a remote network, you need to supply information for the network address, size, and gateway. See the example that follows.

Example: Remote Network Configuration

Opsware DHCP Network Configuration Tool

All values which prompt for an address accept either a IP or a hostname.

Enter network/netmask or network/bits: 192.168.10.0/24

Enter the network gateway: 192.168.10.1

Enter the DHCP Range (start address, stop address)

: 192.168.10.51, 192.168.10.59

Enter the DNS server(s) (comma separated)

: 192.168.2.25, 192.168.2.28

Enter the DNS domain: opsware.com

- 8** If the displayed information is correct, enter `k` to keep the network and return to the main menu.
- 9** At the main menu, to save the information you have entered, enter `s`.
Or
To edit a configured network, enter the corresponding integer and go back to step 3.
Or
To add more networks, enter `a` and go back to step 3.
- 10** To exit the DHCP Network Configuration Tool, enter `e`. You are prompted to start (or restart) the DHCP server process.
- 11** To start (or restart) the DHCP server process, enter `y`. The DHCP Network Configuration Tool displays diagnostic output as part of its startup.

Starting and Stopping the Opware DHCP Server

To start the DHCP server process, enter the following command on the server running the Opware Boot Server:

```
/etc/init.d/opware-sas start dhcpd
```

To stop the DHCP server process, enter the following command on the server running the Opware Boot Server:

```
/etc/init.d/opware-sas stop dhcpd
```

Configuring an Existing ISC DHCP Server for OS Provisioning

You may use an existing ISC DHCP server for OS provisioning instead of the DHCP server included with Opware SAS. An existing ISC DHCP server will work with the provisioning of PXE 2.0 clients, but not with older clients such as PXE 0.99 or 1.0. (These older PXE clients have old PROMS and a PXE bootstrap floppy made with `rbfg.exe`.) The instructions that follow apply to recent versions of an ISC DHCP server, such as version 3.02rc3.

To configure an existing ISC DHCP server, perform the following steps:

- 1** On the server where you installed the Opware Boot Server, you should prevent the Opware DHCP server from running.

On Linux, enter the following command:

```
chkconfig --level 345 dhcpd off
```

On Solaris, enter these commands:

```
rm /etc/rc2.d/S90dhcpd
rm /etc/rc0.d/K30dhcpd
```

- 2** Ensure that the configuration file for the existing ISC DHCP server has the entries shown in: "Example: Configuration File Entries for an Existing ISC DHCP Server" on page 123.

The example is a snippet of the `dhcp.conf` shipped with Opsware SAS, with the addition of `next-server`. This addition tells the PXE client to look for the `tftpserver` on the Opsware core, not on the existing DHCP server.

- 3** If you copy and paste the example, change all of the IP addresses (1 . 2 . 3 . 4) to the IP address of your core.
- 4** Make sure that the DHCP scope for the systems to be provisioned is set up with the required details: DNS server, netmask, default router, DNS domain, and so forth.
- 5** Restart the existing ISC DHCP server.

Example: Configuration File Entries for an Existing ISC DHCP Server

```
#
# declare OPSW site options
#
option space OPSW;
# DANGER WILL ROBINSON - if you change the codes for these
options,
# you'll need to also edit them in the param-request-lists
appearing
# below. Note that in the pxeclient section, you need to specify
the
# values in hex, not in decimal. Also, these values are burned
into
# a couple other files you'll need to edit as well:
# /opt/opsware/boot/tftpboot/pxelinux.cfg/default
# /opt/opsware/boot/jumpstart/Boot/etc/dhcp/inittab
# /opt/opsware/boot/jumpstart/Boot/etc/default/dhcpagent
option OPSW.buildmgr_ip code 186 = ip-address;
option OPSW.buildmgr_port code 187 = unsigned integer 16;

#
# define OPSW site options
#
site-option-space "OPSW";
option OPSW.buildmgr_ip 1.2.3.4;
option OPSW.buildmgr_port 8017;
```

```
#
# declare SUNW jumpstart vendor options (Sun recommended naming)
#
option space SUNW;
option SUNW.SrootIP4 code 2 = ip-address;
option SUNW.SrootNM code 3 = text;
option SUNW.SrootPTH code 4 = text;
option SUNW.SbootFIL code 7 = text;
option SUNW.SinstIP4 code 10 = ip-address;
option SUNW.SinstNM code 11 = text;
option SUNW.SinstPTH code 12 = text;
option SUNW.SsysidCF code 13 = text;
option SUNW.SjumpsCF code 14 = text;
option SUNW.Sterm code 15 = text;

#
# define SUNW jumpstart vendor options
#
class "solaris-sun4u" {
    match option vendor-class-identifier;
    vendor-option-space SUNW;
    next-server 1.2.3.4;
    option SUNW.SrootIP4 1.2.3.4;
    option SUNW.SrootNM "js";
    option SUNW.SrootPTH "/opt/opsware/boot/jumpstart/Boot";
    option SUNW.SinstIP4 1.2.3.4;
    option SUNW.SinstNM "js";
    option SUNW.SjumpsCF "js:/opt/opsware/boot/jumpstart/Conf";
    option SUNW.SsysidCF "js:/opt/opsware/boot/jumpstart/Conf";
    option SUNW.Sterm "vt100";
    option SUNW.SbootFIL "/platform/sun4u/kernel/sparcv9/unix";
    # We use a bogus install path just to give the installer
something to
    # mount for now.
    option SUNW.SinstPTH "/opt/opsware/boot/jumpstart/Boot";
    option dhcp-parameter-request-list 1,3,6,12,15,43,186,187;
}

# Begin dhcptool added SUNW client classes (do not edit)
subclass "solaris-sun4u" "FJSV.GPUU";
subclass "solaris-sun4u" "NATE.s-Note_737S";
subclass "solaris-sun4u" "NATE.s-Note_747S";
subclass "solaris-sun4u" "NATE.s-Note_777S";
subclass "solaris-sun4u" "SUNW.Netra-T12";
subclass "solaris-sun4u" "SUNW.Netra-T4";
subclass "solaris-sun4u" "SUNW.Sun-Blade-100";
subclass "solaris-sun4u" "SUNW.Sun-Blade-1000";
```

```
subclass "solaris-sun4u" "SUNW.Sun-Fire-15000";
subclass "solaris-sun4u" "SUNW.Sun-Fire-280R";
subclass "solaris-sun4u" "SUNW.Sun-Fire-480R";
subclass "solaris-sun4u" "SUNW.Sun-Fire-880";
subclass "solaris-sun4u" "SUNW.Sun-Fire";
subclass "solaris-sun4u" "SUNW.Ultra-1-Engine";
subclass "solaris-sun4u" "SUNW.Ultra-1";
subclass "solaris-sun4u" "SUNW.Ultra-2";
subclass "solaris-sun4u" "SUNW.Ultra-250";
subclass "solaris-sun4u" "SUNW.Ultra-30";
subclass "solaris-sun4u" "SUNW.Ultra-4";
subclass "solaris-sun4u" "SUNW.Ultra-5_10";
subclass "solaris-sun4u" "SUNW.Ultra-60";
subclass "solaris-sun4u" "SUNW.Ultra-80";
subclass "solaris-sun4u" "SUNW.Ultra-Enterprise-10000";
subclass "solaris-sun4u" "SUNW.Ultra-Enterprise";
subclass "solaris-sun4u" "SUNW.UltraAX-MP";
subclass "solaris-sun4u" "SUNW.UltraAX-e";
subclass "solaris-sun4u" "SUNW.UltraAX-e2";
subclass "solaris-sun4u" "SUNW.UltraAX-i2";
subclass "solaris-sun4u" "SUNW.UltraSPARC-IIe-NetraCT-40";
subclass "solaris-sun4u" "SUNW.UltraSPARC-IIe-NetraCT-60";
subclass "solaris-sun4u" "SUNW.UltraSPARC-IIi-Engine";
subclass "solaris-sun4u" "SUNW.UltraSPARC-IIi-Netract";
subclass "solaris-sun4u" "SUNW.UltraSPARC-IIi-cEngine";
subclass "solaris-sun4u" "SUNW.UltraSPARCengine_CP-20";
subclass "solaris-sun4u" "SUNW.UltraSPARCengine_CP-40";
subclass "solaris-sun4u" "SUNW.UltraSPARCengine_CP-60";
subclass "solaris-sun4u" "SUNW.UltraSPARCengine_CP-80";
# End dhcptool added SUNW client classes (do not edit)

#
# declare PXE vendor options
#
option space PXE;
option PXE.mtftp-ip          code 1  = ip-address;
option PXE.mtftp-cport       code 2  = unsigned integer 16;
option PXE.mtftp-sport       code 3  = unsigned integer 16;
option PXE.mtftp-tmout       code 4  = unsigned integer 8;
option PXE.mtftp-delay        code 5  = unsigned integer 8;
option PXE.discovery-control code 6  = unsigned integer 8;
option PXE.discovery-mcast-addr code 7  = ip-address;
option PXE.boot-item          code 71 = unsigned integer 16;

#
# define PXE vendor options
#
```

```
class "pxeclients" {
    match if substring (option vendor-class-identifier, 0, 9) =
    "PXEClient";
    vendor-option-space PXE;
    filename "pxelinux.0";
    next-server 1.2.3.4;
    option vendor-class-identifier "PXEClient";
    # We set the MCAST IP address to 0.0.0.0 to tell the boot ROM
we
    # can't provide multicast TFTP, so it will have to use just
    # plain ol' TFTP instead (address 0.0.0.0 is considered
    # as "no address").
    option PXE.mtftp-ip 0.0.0.0;
    option dhcp-parameter-request-list = concat(dhcp-parameter-
request-list,ba,bb);
}
```

Configuring the MS Windows DHCP Server for OS Provisioning

You may use the MS Windows DHCP server instead of the Opware DHCP server to provision Windows or Linux on PXE 2.0 clients. The MS Windows DHCP server cannot be used during the OS provisioning of the following types of systems:

- Solaris
- PXE 0.99, 1.x clients (These older PXE clients have old PROMS and a PXE bootstrap floppy made with `rbfg.exe`.)

To configure the MS Windows DHCP server for OS Provisioning, perform the following steps:

- 1** On the MS Windows system running the DHCP server, you need to add the option #60, so that it appears in the DHCP scope options. Open a command prompt, and enter the following command:

```
netsh.exe dhcp server add optiondef 60 "PXEClient" STRING
```
- 2** Using the DHCP management snap-in (`dhcpmgmt.msc`), create a scope, which is usually a subnet declaration. In the scope options, #60 should now appear. Check the box, and then add the string `PXEClient`.
- 3** Using the same scope options box, configure options 66 and 67: Click the DHCP option #66 (Boot Server Host Name), and add the full DNS name of the tftp/boot server (for example `core01.test.com`). For option #67 (Bootfile Name), add the boot file name: `pxelinux.0`.

- 4 Make sure that the DHCP scope for the systems to be provisioned is set up with the required details: DNS server, netmask, default router, DNS domain, and so forth.
- 5 At the command prompt, enter the following commands to locate the IP address of the Opware Agent Gateway and the port forward for the Build Manager:


```
netsh.exe dhcp server add optiondef 186 "buildmgr_ip" IPADDRESS
netsh.exe dhcp server add optiondef 187 "buildmgr_port" WORD
```
- 6 Using the DHCP management snap-in (`dhcpcmgmt.msc`), configure the options 186 and 187 to be part of your scope, and give them the appropriate values (IP address of the Opware Agent Gateway and the port forward for the Build Manager, normally 8017).
- 7 Also in the scope, define option 043 (Vendor specific options) as a BINARY type, with the value `01 04 00 00 00 00 ff`. This setting tells the DHCP server to go directly to the tftp server specified in the Boot Server Host Name parameter, and also tells it to not use Multicast TFTP.
- 8 Restart the MS Windows DHCP server.

Configuring the Opware and MS Windows DHCP Servers for OS Provisioning

You can configure the Opware DHCP server to respond only to the OS provisioning requests (that is, from the PXE and Solaris clients), while the MS Windows DHCP server responds to all other requests.

- 1 Add the network subnet to the Opware DHCP server. See “Configuring the Opware DHCP Server for OS Provisioning” on page 120.
- 2 Stop the Opware DHCP server:


```
/etc/init.d/opware-sas stop dhcpd
```
- 3 Make a copy of the Opware DHCP configuration file:


```
cd /etc/opt/opware/dhcpd
cp dhcpd.conf dhcpd.conf.orig
```
- 4 In a text editor, open the Opware DHCP configuration file.
- 5 In the text editor, find the subnet definition you want to configure and comment out (with the # character) these lines:

```
range <IP1> <IP2>;
```

- 6** Immediately after the commented out line (`# range`), enter lines such as:

```
pool {  
    allow members of "solaris-sun4u";  
    allow members of "solaris-sun4us";  
    allow members of "pxeclients";  
    range <IP1> <IP2>;  
}
```

The preceding `pool` statement tells the DHCP server to continue serving the range specified, but only for the three types of clients indicated. (The first two `allow` statements are for Sun machines, the third is for PXE clients). In the preceding `pool` statement, be sure to include the closing brace `}`.

- 7** Repeat the preceding two steps for every subnet you wish to configure.

- 8** In the text editor, save the `dhcpd.conf` file.

- 9** Start the Opware DHCP server:

```
/etc/init.d/opware-sas start dhcpd
```

- 10** Check the logs for DHCP errors. The DHCP service logs with `syslog`. See the `syslog.conf` file to determine how logging has been configured for the Opware DHCP server.

- 11** Make sure that the MS Windows DHCP server subnet/scope declarations are changed to include the build manager DHCP options (code 186 and 187). See “Configuring the MS Windows DHCP Server for OS Provisioning” on page 126.

- 12** Make sure that the MS Windows DHCP server does not include options 43, 60, 66, or 67 in the scope/subnets you are configuring. This will prevent the PXE and Sun jumpstart clients from talking to the MS Windows DHCP server. Instead, they will talk to the Opware DHCP server.

- 13** Make sure that the IP ranges of the MS Windows and Opware DHCP servers don't overlap. As a guideline, the number of IP addresses in a given range should be twice the maximum number of servers that will be provisioned concurrently.

- 14** If the DHCP servers aren't directly connected to the network/subnet of the systems being provisioned, the DHCP requests must be forwarded to both DHCP servers, with the Opware DHCP server being first.

Additional Network Requirements for OS Provisioning

OS Provisioning for Solaris

If you are using OS provisioning for Solaris (JumpStart) on an isolated network, you must have a default gateway (router) available, even if it does not route packets. For Solaris JumpStart to function properly, the IP address of the default gateway must be sent to the installation client that is being provisioned with DHCP. When you use the Opsware DHCP Configuration Tool, a default gateway is properly configured for Solaris because the DHCP Configuration Tool adds the default router appropriately.

Host Name Resolution

For Windows OS provisioning, the host name `buildmgr` should resolve on Windows installation clients.

The Opsware core host names must resolve using the DNS search order and DNS server information that the DHCP server provides. The DHCP server provides the DNS server IP address and the DNS search order. For each subnet you configure with the Opsware DHCP Tool, the DNS domain used by that subnet must have a DNS entry for `buildmgr`.

For example, you could have two subnets with the following domain names:

```
subnet1.example.com  
subnet2.example.com.
```

Therefore, there must be two DNS entries:

```
buildmgr.subnet1.example.com  
buildmgr.subnet2.example.com.
```

The host running the OS Provisioning Media Server must be able to resolve the IP address to the host name (a reverse lookup) of a server being provisioned.

See also “Host and Service Name Resolution Requirements” on page 55.

Open Ports

The server on which the OS is to be provisioned has the same requirements for connectivity to the Opsware core network as a managed server. See “Open Ports” on page 53.

Patch Management on Windows NT 4.0 and Windows 2000

To use the `mbascli.exe` patch utility for patch management on Windows NT 4.0 and Windows 2000, you must first install Internet Explorer 6.0 or later because the `mbascli.exe` patch utility depends on it. This prerequisite is not required for Windows 2003 because IE 6.0 is pre-installed for this operating system.

Creating a Silent Installable Version of IE 6.0 or Later

To create a silent-installable version of IE 6.0 or later, use the Internet Explorer Administrator's Kit (IEAK) for the version of IE that you want to install. For more information on IEAK, see the following URL:

<http://microsoft.com/windows/ieak/default.asp>

Perform the following steps to create a silent installable version of IE 6.0 or later:

- 1** Install IEAK on your desktop system.
- 2** After you install IEAK, start the Internet Explorer Customization Wizard.
- 3** When creating the package, IEAK prompts for a Media Selection option. Select the option Flat (all files in one directory).
- 4** Select the defaults for all other options when you use the wizard.
- 5** After the wizard is complete, zip the contents of the directory it created. This directory contains the silent-installable version of IE.
- 6** To upload the ZIP package into Opware SAS. See the *Opware® SAS User's Guide: Application Automation* for the steps to import software by using the SAS Client.
- 7** Set the following properties for the package when you import it into Opware SAS. See the *Opware® SAS User's Guide: Application Automation* for the steps to edit the properties for a package in the SAS Client.
 - In the Installation Parameters section in the Install Flags field, enter the installation location:
`%SystemDrive%\IE-redist`
 - In the In the Installation Parameters section in the Reboot Required field, select the Yes option.
 - In the Install Scripts section in the Post-Install Script tab, enter this text:
`%SystemDrive%\IE-redist\ie5setup.exe /q:a /r:n`
Where `ie6setup.exe` is the IE 6.x stub installer

The `/q:a` install option specifies quiet install mode, with no user prompts. The `/r:n` install option suppresses restarting the server after IE installation.

- 8** Create a policy in the Software Policies and add the package to the policy. See the *Opware® SAS User's Guide: Application Automation* for the steps to create a software policy and add a package to a software policy.
- 9** Use SAS Client to install the necessary software on a Windows NT 4.0 or Windows 2000 managed server. See the *Opware® SAS User's Guide: Application Automation* for the steps to install software on a server by remediating a software policy onto a managed server.

Adding Instances of the Opware Global File System Server (OGFS) to a Core

To install multiple instances of the OGFS when you install an Opware core, during the Opware Installer interview, specify the IP addresses of the servers on which you plan to install the OGFS and follow the steps for installing an Opware SAS component.

To install additional instances of the OGFS to an existing core, you must edit the following files:

- On the following servers:
 - NFS server storing the user home and tmp directories for the OGFS (the `ogfs.store.host` parameter in the response file)
 - NFS server storing the audit streams for the OGFS (the `ogfs.audit.host` parameter in the response file)

(The default value for both parameters is `theword`)

Edit `/etc/exports` (on Linux) or `/etc/dfs/dfstab` (on Solaris) by adding the IP address of the new OGFS server to allow it to mount the `ogfs.store.path` and `ogfs.audit.path` directories.

See Chapter 5, "Opware Global File System Prompts" on page 94 of this guide for more information.

- On the server that's running the Opware Gateway:

Edit the `/etc/opt/opware/opswgw-cgw0-<dcname>/opswgw.properties` file to add the ingress map for the new OGFS server; for example, add the following line:

```
opswgw.IngressMap=<IP address of the new OGFS host>:HUB
```

- On each server that's running an Opsware Command Center:

Edit the `/etc/opt/opsware/opswgw-lb/opswgw.properties` file by appending:

```
:<IP address of the new OGFS host>:2222
```

To the line:

```
opswgw.LoadBalanceRule
```

Chapter 8: Opsware Multimaster Installation

IN THIS CHAPTER

This section discusses the following topics:

- Multimaster Installation
- Components of Multimaster Installations
- Converting a Core from Standalone to Multimaster
- Adding a Core to a Multimaster Mesh
- Multimaster Post-Installation Tasks

Multimaster Installation

An Opsware multimaster mesh contains two or more cores that communicate with each other. This section refers to the first core you install in a multimaster mesh as the source core. The target core is the second, third, or subsequent core that you install in a multimaster mesh.

The main phases in creating a multimaster mesh of cores are shown in the following steps:

- 1** Install a standalone (source) core.
 - Run the Opsware Installer interview, saving the data you enter at the prompts in a response file.
 - Run the installer again, specifying the response file, on one or more servers to install the Opsware components.
 - See “Installing a Standalone Core” on page 102.
- 2** Convert the standalone core to a multimaster core.
 - Run the Opsware Installer interview with the response file created in the previous step, and then save your answers for this interview in another response file.

- Run the installer again, specifying the latest response file, on one or more servers to add the multimaster components to the source core.
- See “Converting a Core from Standalone to Multimaster” on page 136.

3 Add the new target core to the multimaster mesh.

- On the source core, run the Opware Installer interview with the response file created in the previous step, and then save your answers for this interview in another response file.
- Run the installer again, specifying the latest response file, and instruct the installer to define a new facility.
- Run the installer again to export data from the Model Repository and to create a global response file.
- Copy the export data file and the global response file from the source core server to the target core server.
- On the target core, run the Opware Installer interview with the global response file and save your answers for this interview in another response file.
- Run the installer again, specifying the latest response file, on one or more servers to install the components of the target core.
- See “Adding a Core to a Multimaster Mesh” on page 139.

For a given multimaster mesh, you perform steps 1 and 2 one time only. You perform step 3 every time you want to add another core to the multimaster mesh.

Components of Multimaster Installations

This section discusses the following topics:

- Pre-Existing Core Installations
- Opware Command Center
- Prerequisites for a Multimaster Installation
- TIBCO Rendezvous

Pre-Existing Core Installations

If you installed a standalone core at any secondary facilities and you want to include these facilities in your multimaster mesh, you must perform the following tasks:

- Uninstall the Opware core at the secondary facilities. See “Opware SAS Uninstallation” on page 175 in Chapter 11 for more information.
- Follow the instructions in the section “Multimaster Installation” on page 133.

Opware Command Center

Target facilities (cores) in the multimaster mesh are not required to have an Opware Command Center installed. Instead, you can manage the facility from any site in the multimaster mesh that does have an Opware Command Center installed. You need to install the Opware Command Center only if you want to manage your multimaster mesh locally from that facility or if you want to have a backup Opware Command Center.

TIBCO Rendezvous

In a multimaster mesh, Opware SAS uses the TIBCO Certified Messaging system to synchronize Model Repositories at different facilities.

When you add a core to a multimaster mesh, the Opware Installer automatically configures the TIBCO Rendezvous routing daemon (`trvd`). For more information, see “TIBCO Rendezvous Configuration for Multimaster” on page 181.

Prerequisites for a Multimaster Installation

Perform the following tasks in preparation for installing a multimaster core:

- Plan your Opware System deployment. When planning for a core, you must decide whether you want to install the core components on a single server or on multiple servers. See Chapter 1, “Opware SAS Architecture” and “Opware Core Scalability for Performance” on page 43.
- Perform the pre-installation administration tasks such as configuring the network. See Chapter 3, “Pre-Installation Requirements.”
- Gather information in preparation for the Opware Installer interview. This information includes the name and ID of the facility for the core. See Chapter 5, “Prerequisite Information for the Installer Interview.”
- Verify that every Opware core server has a unique IP address within the entire multimaster mesh.

- After you synchronize the time on all servers within a facility, synchronize the time between the facilities in the multimaster mesh. Synchronize the time with an external time-server that uses Network Time Protocol (NTP) so that all servers are using the same Coordinated Universal Time (UTC).
- Verify that the multimaster installation meets same network requirements as a standalone installation, except that each core must be on a different Local Area Network (LAN or VLAN). The cores must be in different broadcast domains.
- Make sure that each core in a mesh has a different subdomain so that managed servers can resolve the unqualified host names `spin`, `way`, and `theword`.
- Verify that the `tnsnames.ora` file on the source core contain entries for every Model Repository in the mesh. If the `tnsnames.ora` file of the source core does not contain an entry for the target core, then multimaster conflicts will occur.

Converting a Core from Standalone to Multimaster

This section describes how to convert an Opware core from standalone to multimaster. Throughout this section, the core to be converted is referred to as the source core. (If you already have a multimaster mesh and want to add an additional core, go to the section “Adding a Core to a Multimaster Mesh” on page 139.)

Perform the following steps to convert a core from standalone to multimaster:

- 1** Obtain the Opware SAS installation media for this release.
See “Installation Media for the Opware Installer” on page 97, including the recommendation, “Copying the DVD to a Local Disk.”
- 2** On each server of the source core, mount the Product Software DVD or NFS-mount the directory that contains a copy of the DVD contents.
The Opware Installer must have read/write root access to the directories where it installs Opware components, even NFS-mounted network appliances.
- 3** On the Model Repository server in the source core, log in as root.
- 4** Change to the root directory:
`cd /`
- 5** Invoke the Opware Installer with the `-r` (response file) and the `--interview` options. For example:


```
/opware_system/opware_installer/install_opware.sh -r
/usr/tmp/oiresponse.stand_single --interview
```

You must specify the full path to the script. The directory path in the preceding command indicates that you copied the Opware SAS Product Software DVD to a local disk or network share using the required directory structure.

You should run the Opware Installer with the response file that you created when you installed the source core. If this response file is not available, invoke the Opware Installer with no command line options, and the interview will automatically start.

The Opware Installer displays the following options:

Welcome to the Opware Installer. Please select one of the following installation options:

```
1 - Standalone Installation: Standalone Opware Core
2 - Multimaster Installation: First Core (convert from
standalone)
3 - Multimaster Installation: Define New Facility; Export
Model Repository
4 - Multimaster Installation: Additional Core
```

6 At the installation options prompt, select the following option:

```
2 - Multimaster Installation: First Core (convert from
standalone)
```

7 At the interview mode prompt, select one of the following options:

```
1 - Simple Interview Mode
2 - Advanced Interview Mode
```

Option 1 is for using default values for many of the configuration parameters. Option 2 is for specifying all configuration parameters during the interview.

8 Respond to the interview prompts.

The installer displays default values in square brackets [].

See “Required Information for Running the Installer Interview” on page 75.

9 Decide if you want to finish the interview.

When you enter all of the required information, the Opware Installer displays this message:

```
All parameters have values. Do you wish to finish the
interview (y/n):
```

If you are satisfied with your answers, press y.

If you want to review or change your answers, press n. The installer displays the prompts again, showing in brackets [] the values that you previously entered.

10 Create the response file.

When you are finished with the interview, the installer prompts you for the name of the response file:

```
Name of response file to write  
[/usr/tmp/oiresponse.stand_to_mm]
```

The response file is a text file that contains the answers you entered during the interview. You can enter the name of the response file or accept the default. In either case, write down the name of the response file. Note that the default file name corresponds to the type of installation.

11 The Opware Installer prompts you to indicate whether you want to continue the installation by using the response file. Select one of the following options:

- If you are satisfied with the responses you entered in the interview and you are ready to install the Model Repository Multimaster Additions now, enter y to continue.
- If you do not want to install the Model Repository Multimaster Additions now, enter n.

12 If you entered y in the previous step, skip this step. If you entered n in the previous step, invoke the Opware Installer with the -r option to specify the response file created by the latest interview. For example:

```
/opware_system/opware_installer/install_opware.sh -r  
/usr/tmp/oiresponse.stand_to_mm
```

13 At the components prompt, select one or more components to install:

```
Welcome to the Opware Installer.  
Please select the components to install.  
1 ( ) Model Repository (truth), Multimaster Additions  
2 ( ) Data Access Engine (spin), Multimaster Component  
3 ( ) Multimaster Infrastructure Components (vault)  
4 ( ) Command Engine (way), Multimaster Component  
5 ( ) Software Repository (word), Multimaster Component  
6 ( ) Opware Global Filesystem, Multimaster Component  
7 ( ) Opware Command Center (OCC), Multimaster Component  
Enter a component number to toggle ('a' for all, 'n' for  
none).  
When ready, press 'c' to continue, or 'q' to quit.
```

Selection:

You must install the components in the order they are listed. For example, you must install the Model Repository Multimaster Additions first.

If you are installing all of the components on a single server, then you can enter a for all. If you do not select a, then you must run the Opsware Installer again (as shown in the preceding step) and select the remaining components.

- 14** If you are installing the components on multiple servers, follow the instructions in this step. (If you are installing the components on a single server, skip this step.)

Copy the response file generated by the installer interview to all other servers in the source core.

On each server in the source core, run the Opsware Installer with the `-r` option, as shown in step 12. Select and install the remaining components from the menu shown in step 13.

You must install each multimaster addition on the same server running the corresponding standalone component. For example, install the Model Repository Multimaster Additions on the server running the standalone Model Repository, and install the Data Access Engine Multimaster Component on the server running the standalone Data Access Engine. Although not required, the Model Repository Multimaster Component (vault) is usually installed on the same server as the Model Repository.

- 15** Follow the instructions in the section “Adding a Core to a Multimaster Mesh” on page 139.

Adding a Core to a Multimaster Mesh



Before proceeding with the installation, follow the instructions in “Prerequisites for a Multimaster Installation” on page 135.

This section describes how to add a new Opsware core to a multimaster mesh. Throughout this section, the first core in the mesh is referred to as the source core. The new core that you are adding is called the target core. (If you do not have a multimaster mesh, you are reading the wrong section; go to the section “Converting a Core from Standalone to Multimaster” on page 136.)

In an Opsware SAS core, the Opsware Model Repository uses an Oracle database. This section provides the instructions for installing an Opsware SAS core with Oracle 10g by using the Opsware Installer.

For information about installing a Opsware SAS core by using an existing Oracle database, contact your Opsware support representative.

Perform the following steps to add a new core to a multimaster mesh:

- 1** Obtain the Opsware SAS installation media for this release.
See “Installation Media for the Opsware Installer” on page 97, including the recommendation, “Copying the DVD to a Local Disk.”
- 2** On the Model Repository server of the source core and on each server of the target core, mount the Product Software DVD or NFS-mount the directory that contains a copy of the DVD contents.

The Opsware Installer must have read/write root access to the directories where it installs Opsware components, even NFS-mounted network appliances.

- 3** On the Model Repository server in the source core, invoke the Opsware Installer with the `-r` (response file) and the `--interview` options. For example:

```
/opsware_system/opsware_installer/install_opsware.sh -r  
/usr/tmp/oiresponse.stand_to_mm --interview
```

You must specify the response file created when you converted the core from standalone to multimaster.

The Opsware Installer displays the following options:

```
Welcome to the Opsware Installer. Please select one of the  
following installation options:
```

```
1 - Standalone Installation: Standalone Opsware Core  
2 - Multimaster Installation: First Core (convert from  
standalone)  
3 - Multimaster Installation: Define New Facility; Export  
Model Repository  
4 - Multimaster Installation: Additional Core
```

4 At the installation options prompt, select the following option:
3 - Multimaster Installation: Define New Facility; Export Model Repository

5 At the interview mode prompt, select one of the following options:
1 - Simple Interview Mode
2 - Advanced Interview Mode

Option 1 is for using default values for many of the configuration parameters. Option 2 is for specifying all configuration parameters during the interview.

6 Respond to the interview prompts.

The installer displays default values in square brackets [].

For the short name of the target core (`slaveTruth.dcNm` parameter), enter a new facility name. This name must be unique within the multimaster mesh.

See “Required Information for Running the Installer Interview” on page 75.

7 Decide if you want to finish the interview.

When you enter all of the required information, the Opsware Installer displays this message:

```
All parameters have values. Do you wish to finish the
interview (y/n):
```

If you are satisfied with your answers, press y.

If you want to review or change your answers, press n. The installer displays the prompts again, showing in brackets [] the values that you previously entered.

8 Create the response file.

When you are finished with the interview, the installer prompts you for the name of the response file:

```
Name of response file to write
[/usr/tmp/oiresponse.add_dc_to_mesh]
```

The response file is a text file that contains the answers you entered during the interview. You can enter the name of the response file or accept the default. In either case, write down the name of the response file. Note that the default file name corresponds to the type of installation.

9 The Opsware Installer prompts you to indicate whether you want to continue the installation by using the response file. Select one of the following options:

- If the Opsware Gateway in the source core is on a different server than the Model Repository, enter `n`. Copy the response file to the server with the Opsware Gateway and go on to the next step.
- If you are satisfied with the responses you entered in the interview and you are ready to define the new facility now, enter `y` to continue.
- If you do not want to define the new facility now, enter `n`.

10 If you entered `y` in the previous step, skip this step. If you entered `n` in the previous step, log into the server running the Opsware Gateway and invoke the installer with the `-r` option. Be sure to specify the response file created by the latest interview. For example:

```
/opsware_system/opsware_installer/install_opsware.sh -r  
/usr/tmp/oiresponse.add_dc_to_mesh
```

11 At the components prompt, select the following option:

```
1 ( ) Define New Facility
```

Wait for the installer to finish this operation before going on to the next step. The Opsware Installer enters the target facility in the Model Repository of the source core, automatically generating the target facility's ID.

12 Find the ID of the target facility.

To find the facility ID, perform the following steps:

- Log into the Opsware Command Center as the `admin` user at the source facility.
- From the navigation panel, select Facilities under Environment.
- Click the link for the target facility. Write down the facility ID.

In step 13 through step 21, you perform the tasks for exporting data from the Model Repository of the source core.

If you are adding a third (or more) core to a multimaster mesh, you can export data from a core other than the original source core. In this case, the instructions are slightly different, as noted in step 15 on page 143 and step 38 on page 148.

13 On the servers where the Opsware Command Center and the Opsware Global File System Server (OGFS or hub) are installed, stop the Web Services Data Access Engine (`twist`) by entering the following command:

```
/etc/init.d/opsware-sas stop twist
```

- 14** On the servers where the Data Access Engine (spin) is installed, stop the engine by entering the following command:

```
/etc/init.d/opware-sas stop spin
```

If the Opware Command Center and the Data Access Engine are installed on different servers, you must also run the preceding command on the Opware Command Center server.

- 15** On the server running the Model Repository Multimaster Component, wait for all transactions to be published by examining the `/var/log/opware/vault/log` file.

If the log contains successive entries “QUERIED THE DATABASE” and does not contain recent “SENDING TRANSACTION” entries, the transactions from the installation have been published.

If you are going to export data from a core other than the original source core, wait for the transactions to propagate to the core that will be exported before performing step 18 on page 143.

- 16** On the server where the Model Repository Multimaster Component (vault) is installed, stop the engine by entering the following command:

```
/etc/init.d/opware-sas stop vaultdaemon
```

- 17** Log into the server running the Model Repository and invoke the installer with the `-r` option to specify the response file created by the latest interview. For example:

```
/opware_system/opware_installer/install_opware.sh -r
/usr/tmp/oiresponse.add_dc_to_mesh
```

- 18** At the components prompt, select the following option:

```
2 ( ) Export Model Repository (truth)
```

The installer exports the data from the Model Repository into the `truth_data.tar.gz` file, which by default resides in the directory `/var/opt/opware/truth`. (You specified this directory at the `truth.dest` prompt of the interview.)

Depending on the amount of data, the export might take 20 minutes or more. To track the progress of the export in a different window, run the following command.

```
tail -f /var/log/opware/install_opware/truth
/truth_exp<number>.log
```

- 19** On the source core servers where the Data Access Engine (spin) is installed, start the engine by entering the following command:

```
/etc/init.d/opsware-sas start spin
```

If the Opware Command Center and the Data Access Engine are installed on different servers, you must also run the preceding command on the Opware Command Center server.

- 20** On the servers where the Opware Command Center and the Opware Global File System Server (OGFS or hub) are installed, start the Web Services Data Access Engine (twist) by entering the following command:

```
/etc/init.d/opsware-sas start twist
```

- 21** On the server where the Model Repository Multimaster Component (vault) is installed, start the engine by entering the following command:

```
/etc/init.d/opsware-sas start vaultdaemon
```

Examine the logs for the Model Repository Multimaster Component to ensure that it started properly. These logs are located in the following directory:

```
/var/log/opsware/vault
```

The log files are named `log`, `log.1`, `log.2`, `log.3`, and so forth.

- 22** Copy the Model Repository export file (`truth_data.tar.gz`) to the server where you will install the Model Repository in the target core.

The Unix `oracle` user needs read access to the `truth_data.tar.gz` file on the Model Repository host in the target core.

- 23** Copy the global response file (`oiresponse.global`) from the source core server of the Model Repository to the target core server on which you will install the new Model Repository.

On the source core, the `oiresponse.global` file resides in the same directory as the Model Repository export file. The default directory is `/var/opt/opsware/truth`.

- 24** On the target core servers, make the following directory:

```
mkdir -p /var/opt/opsware/crypto/cadb/realm
```

- 25** Copy the database of cryptographic material and the Unix Tar file Gzipped from the source core server that is running the Model Repository to every target core server. The database of cryptographic material and the Unix Tar file Gzipped are in the following files:


```
/var/opt/opware/crypto/cadb/realm/opware-crypto.db.e
/var/opt/opware/crypto/cadb/realm/opware-crypto.tgz.e
```

The full path name of the file on the target core servers must match the preceding lines. The root user requires read access to the directory and files.

- 26** Log into the target core server on which you will install the Model Repository and invoke the Opware Installer. Specify the `-r oiresponse.global` file and the `--interview` options. For example:

```
/opware_system/opware_installer/install_opware.sh -r
/usr/tmp/oirresponse.global --interview
```

Be sure to specify the global response file that you copied to the target core.

The Opware Installer displays following options:

Welcome to the Opware Installer. Please select one of the following installation options:

```
1 - Standalone Installation: Standalone Opware Core
2 - Multimaster Installation: First Core (convert from
standalone)
3 - Multimaster Installation: Define New Facility; Export
Model Repository
4 - Multimaster Installation: Additional Core
```

- 27** At the installation options prompt, select the following option:

```
4 - Multimaster Installation: Additional Core
```

- 28** At the interview mode prompt, select one of the following options:

```
1 - Simple Interview Mode
2 - Advanced Interview Mode
```

Option 1 is for using default values for many of the configuration parameters. Option 2 is for specifying all configuration parameters during the interview.

- 29** At the database configuration option prompt, select the following option:

```
1 - Install Oracle with Opware
```

For information about installing an Opware SAS core by using option 2 (“Use Existing Oracle Database”), contact your Opware support representative. When you use an existing Oracle database, you must configure the Oracle database instance correctly to work with the Opware SAS core.

- 30** Respond to the interview prompts.

The installer displays default values in square brackets []. Unless you have changed the source core, do not change the values that were in the global response file you copied from the source core. Note the following requirements for the prompts:

- The facility ID, short name, and subdomain must match the values generated when the target facility was defined in the source core. You wrote down the facility ID in step 12 on page 142.
- The authorization domain must match the value provided for the source core.
- The path to the data export file, `truth_data.tar.gz`, in the target core must match the path you used when copying the file from the source core.
- The path for the OS provisioning media must already exist on the server where you will install the OS Provisioning Media Server component.

31 Decide if you want to finish the interview.

When you enter all of the required information, the Opware Installer displays this message:

```
All parameters have values. Do you wish to finish the
interview (y/n):
```

If you are satisfied with your answers, press y.

If you want to review or change your answers, press n. The installer displays the prompts again, showing in brackets [] the values that you previously entered.

32 Create the response file.

When you are finished with the interview, the installer prompts you for the name of the response file:

```
Name of response file to write
[/usr/tmp/oiresponse.mmm_subs]
```

The response file is a text file that contains the answers you entered during the interview. You can enter the name of the response file or accept the default. In either case, write down the name of the response file. Note that the default file name corresponds to the type of installation.

33 The Opware Installer prompts you to indicate whether you want to continue the installation by using the response file. Select one of the following options:

- If you are satisfied with the responses you entered in the interview and you are ready to install the Model Repository now, enter y to continue.

- If you do not want to install the Model Repository now, enter `n`.

34 If you entered `y` in the previous step, skip this step. If you entered `n` in the previous step, invoke the Opware Installer with the `-r` option to specify the response file created by the interview. For example:

```
/opware_system/opware_installer/install_opware.sh -r
/usr/tmp/oiresponse.mmm_subs
```

35 At the components prompt, select one or more components to install:

```
Welcome to the Opware Installer.
Please select the components to install.
1 ( ) Oracle RDBMS
2 ( ) Model Repository (truth), Secondary Core
3 ( ) Data Access Engine (spin), Multimaster Component
4 ( ) Multimaster Infrastructure Components (vault)
5 ( ) Command Engine (way), Multimaster Component
6 ( ) Software Repository (word), Multimaster Component
7 ( ) Opware Global Filesystem, Multimaster Component
8 ( ) Opware Global Filesystem Server (OGFS)
9 ( ) Opware Command Center (OCC), Multimaster Component
10 ( ) OS Provisioning Media Server
11 ( ) OS Provisioning Build Manager
12 ( ) Opware Gateway, Secondary Core
13 ( ) OS Provisioning Boot Server
Enter a component number to toggle ('a' for all, 'n' for
none).
When ready, press 'c' to continue, or 'q' to quit.
```

Selection:

You must install the components in the order they are listed. For example, you must install the Model Repository first.

If you are installing all of the components on a single server, then you may enter `a` for all. If you do not select `a`, then you must run the Opware Installer again (as shown in the preceding step) and select the remaining components. (If you are installing the components on multiple servers, see the next step.)

36 If you are installing the components on multiple servers, follow the instructions in this step. (If you are installing the components on a single server, skip this step.)

Copy the response file generated by the installer interview to all other servers in this core.

Copy the `tnsnames.ora` file from the server with the Model Repository to the other core servers. The directory path for the file must be the same on all core servers. (By default, `tnsnames.ora` is in the `/var/opt/oracle` directory.)

On each server in this core, run the Opware Installer with the `-r` option, as shown in step 34. Select and install the remaining components from the menu shown in step 35.

You must install the Opware Documentation component on the server where you install the Opware Command Center component.

If the Model Repository exists on a server with no other Opware components installed on it, you must install an Opware Agent on that server. See the *Opware® SAS User's Guide* for instructions.

37 (Optional) If you are distributing the core components across multiple servers, you can install additional instances of the following components:

- Data Access Engine

If you install more than one Data Access Engine, then you must perform the procedure described in “Reassigning the Data Access Engine to a Secondary Role” in the *Opware® SAS Administration Guide*.

- OS Provisioning Media Server
- Opware Command Center
- Opware Global File System

To install multiple instances of the OGFS when you install an Opware core, during the Opware Installer interview, specify the IP addresses of the servers on which you plan to install the OGFS.

To install additional instances of the OGFS to an existing core, you must perform manual steps. See Chapter 7, “Adding Instances of the Opware Global File System Server (OGFS) to a Core” on page 131 of this guide for more information.

38 If you exported data from a core other than the original source core, you might need to configure TIBCO manually.

By default, the target core will try to connect to the original source core. If you want the target core to connect to a different core then you must configure TIBCO manually and edit the Opware Gateway properties file. For instructions, see “Adding a TIBCO Rendezvous Neighbor” on page 183.

39 Perform the tasks in Chapter 7, “Post-Installation Tasks” on page 111 of this guide.

40 Perform the tasks in the following section.

Multimaster Post-Installation Tasks

After you add a new core to a multimaster mesh, perform the tasks described in this section.

Associating Customers with a New Facility

Associate the appropriate customers with each new facility so that servers managed at that facility are associated with the correct customers accounts. For more information, see the Customer Account Administration section of the *Opware® SAS Configuration Guide*.

Updating Permissions for New Facilities

After you add new facilities to your multimaster mesh, your Opware users will not have the required permissions to access these new facilities. To grant access, you must assign the required permissions to the user groups. For more information, see the User Group and Setup section of the *Opware® SAS Configuration Guide*.

Verifying Multimaster Transaction Traffic

Perform the following steps to verify multimaster transaction traffic with the target facility:

- 1** Log into the Opware Command Center as a user that belongs to the Opware System Administrators group.
- 2** From the navigation panel, click Multimaster Tools under Administration. The State View window appears.
- 3** In the State View Window, note the color of the status box beside each transaction.

A transaction is a unit of change to a Model Repository database that consists of one or more updates to rows and has a globally unique transaction ID. If the transactions with the target facility are green, the new Opware core is integrated into the multimaster mesh. It is normal for some of the transactions to have an orange status (not sent) for a while.

- 4** Click **Refresh** to refresh the cached data.

For more information, see the Opware Multimaster Mesh Administration section in the *Opware® SAS Administration Guide*.

Chapter 9: Opsware Satellite Installation

IN THIS CHAPTER

This section discusses the following topics:

- Overview of Satellite Installation
- Satellite Requirements
- Gateway Configuration for a Satellite
- Satellite Installation
- Post-Installation Tasks for a Satellite

Overview of Satellite Installation

An Opsware Satellite manages servers in a remote data center. The following steps provide an overview of the Satellite installation process. For detailed instructions, see “Satellite Installation” on page 162.

- 1** Obtain the Opsware SAS installation DVDs.
- 2** Run the Opsware Installer (`install_opsware.sh` script) in interview mode. The interviewer prompts you for information about your environment and saves the information in a response file.
- 3** Run the Opsware Installer and select the Opsware Gateway from the list of components to install. The Opsware Installer launches the Opsware Gateway Installer.
- 4** Respond to the prompts of the Opsware Gateway Installer.
- 5** Run the Opsware Installer (`install_opsware.sh` script) and select the other components to install.

Satellite Requirements

Before you install an Opsware Satellite, verify that the requirements detailed in the following sections are met.

Open Ports Required for a Satellite

The ports listed in Table 9-1 must be open for the Opsware Gateway in a Satellite. The ports in the table are the default values. (You may select other values during the installation.)

Table 9-1: Open Ports for a Satellite Gateway

| PORT | PROPERTY NAME IN OPSWARE GATEWAY PROPERTIES FILE | DESCRIPTION |
|------|--|--|
| 2001 | <code>opswgw.TunnelDst</code> | The port for a tunnel end-point listener. This port will be used if you install other Gateways that tunnel to the Gateway on this Satellite. |
| 3001 | <code>opswgw.ProxyPort</code> | The proxy port on which the Agents contact the Gateway. |
| 4040 | <code>opswgw.IdentPort</code> | The port of the Gateway's <code>ident</code> service, which is used by the Software Repository Cache. |

If you are going to install the OS Provisioning Boot Server and Media Server in the Satellite, then additional ports must be open. For a list of these ports, see Table 3-2 on page 54.

Entries Required in `/etc/hosts` for a Satellite

The Software Repository Cache of the Satellite requires the following entries in the `/etc/hosts` file:

```
127.0.0.1 theword
127.0.0.1 wordcache
```

Required Packages for SuSE Linux Enterprise Server 9

For a Satellite running this version of Linux, the following packages must be installed:

- `nfs-utils` (for OS Provisioning Boot Server)

- `xinetd` (for `tftp`)
- `sharutils` (for `uuencode` and `uudecode` in ADT)
- `compat-2004.7.1-1.2` (for ADT, `compat` includes `libstdc++`)

Other Requirements for a Satellite

The following requirements must also be met:

- The Satellite server meets the requirements listed in “Supported Operating Systems” on page 39. The supported operating systems for the OS Provisioning components are not the same as those for the other Satellite components (Gateway and Software Repository Cache).
- The Satellite server must have the necessary packages listed in “Operating System Requirements” on page 49.
- The Opware core for this Satellite is up and running.
- The Satellite server must have network connectivity to the server running the core Gateway.
- In the Opware Command Center for the core, you can log in as a member of the Administrators group (`admin`) and as a member of a group that has the Manage Gateway permission.
- You have root access on the core server so that you can copy the database of cryptographic material from the core to the Satellite server.
- The Satellite server uses UTC, as described in “Time and Locale Requirements” on page 61. The time of the Satellite server must be synchronized with the core server.
- When using network storage for the Software Repository Cache, the network storage configuration must allow root write access over NFS to the directories where the Software Repository Cache is to be installed.
- If you are going to install the OS Provisioning Boot Server and Media Server in the Satellite, then see the requirements in “DHCP Proxying” on page 56.
- You know how to edit files with the `vi` editor. The Opware Gateway Installer launches the `vi` editor, which you will use to edit a properties file.

Gateway Configuration for a Satellite

This section illustrates various Satellite topologies and the corresponding settings in the Gateway properties files. In the diagrams, the arrows between Gateways represent tunnels. (A tunnel is a TCP connection between two Gateways that carries multiplexed TCP or UDP connections.) The boxes labelled with the letter "A" designate managed servers, which run Opware Agents.

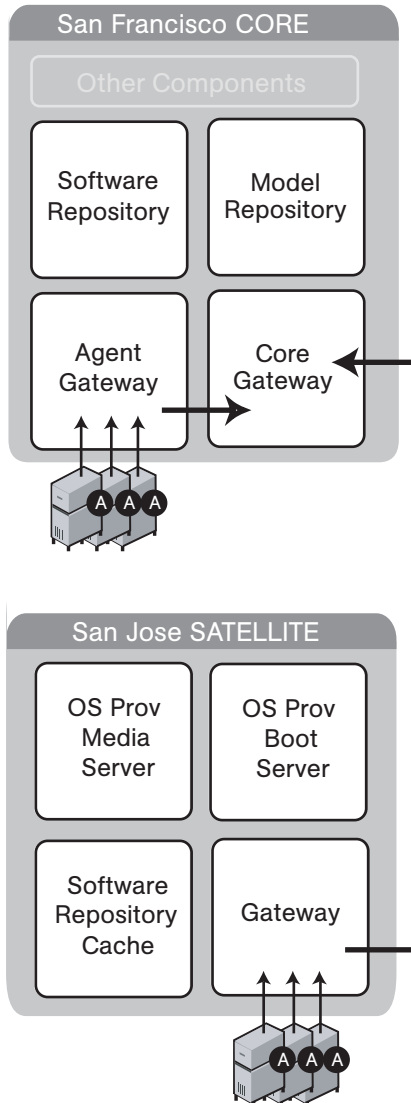
Satellite with a Standalone Core

Figure 9-1 shows a single Opware Satellite that has a tunnel to a standalone core. In this example, the main facility is in San Francisco, and a smaller remote facility is in San Jose.

The core is made up of several components, including the Software Repository, the Model Repository, and two gateways. The figure does not show other required core components, such as the Command Engine, but indicates them with an ellipsis (...) button. When you install a standalone core, the Opware Installer creates both the Agent and core Gateways. The Agents in the San Francisco facility communicate with the core through the Agent Gateway. The Agents in the San Jose facility connect to the San Francisco core via TCP connections to the Satellite Gateway.

In a Satellite, the Software Repository Cache and Gateway components are required. The Software Repository Cache contains local copies of software packages to be installed on managed servers in the Satellite. The Gateway multiplexes connections into and out of the Satellite via one or more tunnels. Optionally, a Satellite can contain the OS Provisioning Boot Server and Media Server components.

Figure 9-1: Single Satellite With a Standalone Core



The following listing shows a few entries in the Gateway properties file of the San Jose Satellite.

In the properties file, the `opswgw.GWAddress` specifies the IP address or host name where the Satellite Gateway runs. When a new Gateway is added to a realm, the value of the `opswgw.GWAddress` is dynamically added to the list of Gateways that Agents in the

realm can communicate with. (A realm is a routable group of IP addresses.) The Agent installer and the `opswgw.GWAddress` must both specify either IP addresses or host names. For example, if the Agent installer specifies an IP address in its `opsw_gw_addr_list` option, then the `opswgw.GWAddress` must also specify an IP address, not a host name. If host names are used, they must be resolvable (with DNS or `/etc/hosts`) by the Agents that contact this Gateway. Specifying IP addresses is recommended because it is less error prone. (This document shows host names in the example diagrams and listings because they are easier to read.)

The `opswgw.Realm` specifies the realm of the Gateway. A realm is a logical name for a group of IP addresses that can be contacted by a particular set of Gateways. Realms enable Opware SAS to manage servers with overlapping IP addresses. (This situation can occur when the servers in a remote facility are behind NAT devices or firewalls.) The realm plus the IP address uniquely identifies a managed server. Servers with overlapping IP addresses must reside in separate realms.

The `opswgw.TunnelSrc` has five parameters. The first two parameters identify the remote host (`sanfran.myops.com`) and port (2001) where the core Gateway listens for connections. Note that the host and port of the `opswgw.TunnelSrc` in the Satellite must match those of the `opswgw.TunnelDst` in the core. The next two parameters of `opswgw.TunnelSrc` specify the cost and bandwidth of the tunnel. (See “Configuring Routing (Cost)” on page 158 and “Limiting Bandwidth” on page 162.) The last parameter (`.../opswgw.pem`) is a certificate file in the Privacy Enhanced Mail (PEM) format. If you specify the certificate file, the data transmitted through the tunnel will be encrypted using SSL. The header of the certificate file includes the cipher choice and authentication options.

The `opswgw.DoNotRouteService` and `opswgw.HijackService` properties are required for this Satellite Gateway because the Satellite includes a Software Repository Cache. With these properties, if an Agent has a request for the Software Repository, the Satellite Gateway routes the request to the local Software Repository Cache.

The `opswgw.ProxyPort` identifies the port on the Satellite through which the Agents contact the Gateway. The `opswgw.IdentPort` is for an identity service used by the Software Repository Cache.

Typically, you'll use the default ports for the properties. However, you must enter the hosts for the `opswgw.GWAddress` and `opswgw.TunnelSrc` properties. The following listing shows some of the entries in the Gateway properties file for the San Jose Satellite. (Although the `opswgw.TunnelSrc` entry wraps around to the next line in this listing, in the actual properties file the entry is on a single line.)

```
opswgw.Gateway=SanJose
opswgw.Realm=SanJose
opswgw.GWAddress=sanjose.myops.com
opswgw.TunnelSrc=sanfran.myops.com:2001:10:0:/var/opt/opsware/
crypto/SanJose/opswgw.pem
opswgw.DoNotRouteService=theword:1003
opswgw.DoNotRouteService=127.0.0.1:1003
opswgw.HijackService=wordcache:1003
opswgw.ProxyPort=3001
opswgw.IdentPort=4040
```

The following lines are from the core Gateway properties file of the San Francisco facility:

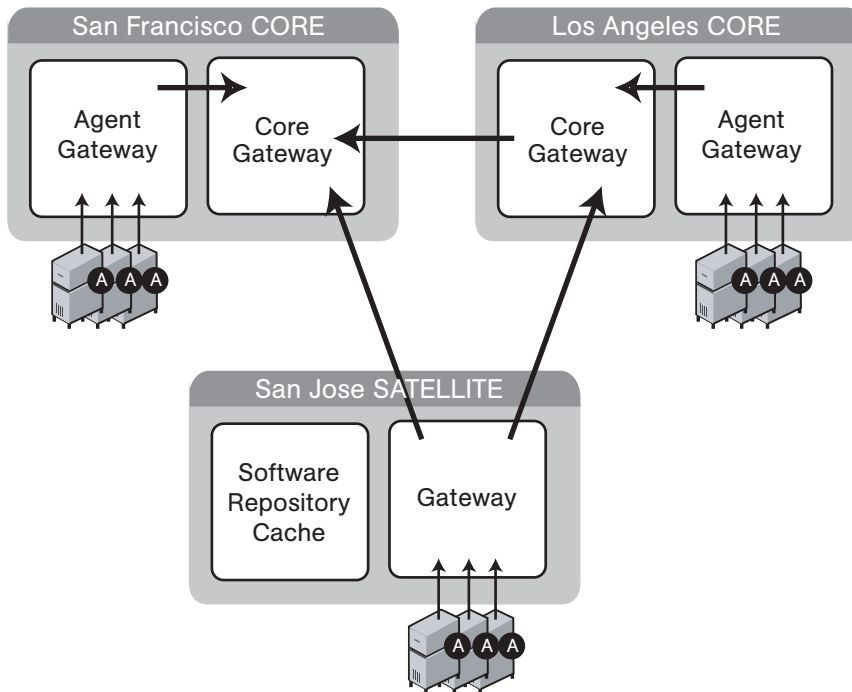
```
opswgw.Gateway=cgw0-SanFrancisco
opswgw.Realm=SanFrancisco
opswgw.TunnelDst=2001:/var/opt/opsware/crypto/cgw0-
SanFrancisco/opswgw.pem
```

Satellite in a Multimaster Mesh

Figure 9-2 shows two cores, San Francisco and Los Angeles, in a multimaster mesh. The multimaster traffic passes through the core Gateways. The Gateway in the San Jose Satellite points to both core Gateways. In this example, the communication link between the San Jose and San Francisco facilities is the fastest and has the most bandwidth. During normal operations, the servers in San Jose are managed by the San Francisco

core. If the connection between San Jose and San Francisco fails, then the Gateway in San Jose will communicate instead with the core in Los Angeles. (See “Configuring Routing (Cost)” on page 158.)

Figure 9-2: Single Satellite in a MultiMaster Mesh



The lines that follow are from the properties file of the Satellite Gateway in San Jose. The first `opswgw.TunnelSrc` property points to the San Francisco Gateway; the second one points to the Los Angeles Gateway. Both lines indicate that the core Gateways use the default port (2001) to listen for connections.

```

opswgw.Gateway=SanJose
opswgw.Realm=SanJose
opswgw.TunnelSrc=sanfran.myops.com:2001:100:0:/var/opt/opsware/
crypto/SanJose/opswgw.pem
opswgw.TunnelSrc=losang.myops.com:2001:200:0:/var/opt/opsware/
crypto/SanJose/opswgw.pem
  
```

Configuring Routing (Cost)

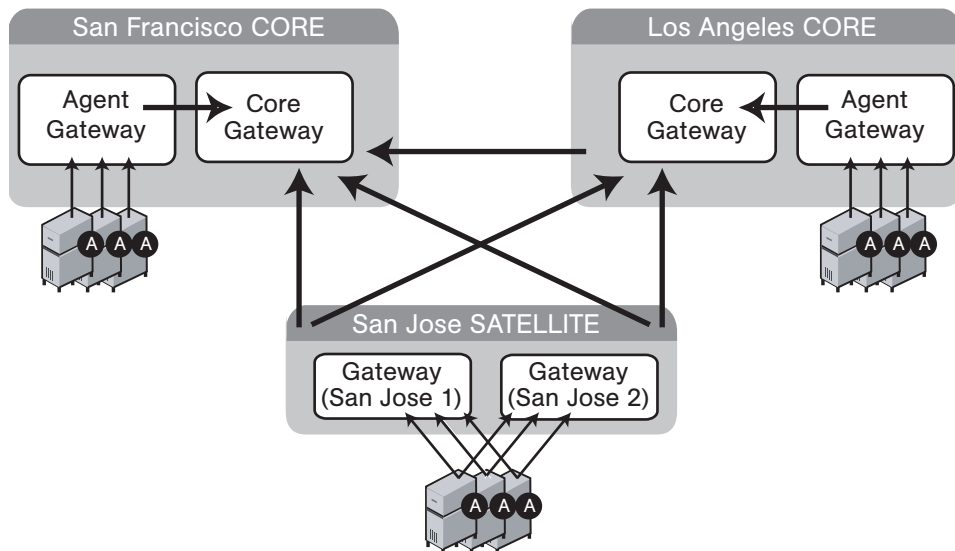
A Satellite Gateway routes traffic to only one core Gateway at any given time. The Gateway chooses the route with the lowest cost. The cost is the third parameter of the `opswgw.TunnelSrc` property. In the preceding listing, the `opswgw.TunnelSrc`

properties specify that the cost from San Jose to San Francisco is 100 and the cost between San Jose and Los Angeles is 200. Therefore, the Satellite Gateway will use the connection to San Francisco, unless for some reason that connection becomes unavailable.

Multiple Gateways in a Satellite

The topology shown in Figure 9-3 provides failover capability in two ways. First, each Gateway in the San Jose Satellite tunnels to both core Gateways. If one core becomes unavailable, the other core can manage the servers in the Satellite. Second, the Agents in the San Jose Satellite point to both Satellite Gateways. If one Satellite Gateway becomes unavailable, the Agents on the managed servers can communicate with a core Gateway via the other Satellite Gateway. Both Gateways in San Jose must belong to the same realm. An Agent can communicate with any Gateway in the same realm.

Figure 9-3: Multiple Gateways in a Satellite



The following lines are from the core Gateway properties file of the San Francisco facility:

```
opswgw.Gateway=cgw0-SanFrancisco
opswgw.Realm=SanFrancisco
opswgw.TunnelDst=2001:/var/opt/opsware/crypto/cgw0-
SanFrancisco/opswgw.pem
```

The core Gateway properties file of the Los Angeles facility has similar entries:

```
opswgw.Gateway=cgw0-LosAngeles
opswgw.Realm=LosAngeles
```

```
opswgw.TunnelDst=2001:/var/opt/opsware/crypto/cgw0-LosAngeles/  
opswgw.pem  
opswgw.TunnelSrc=sanfran.myops.com:2001:1:0:/var/opt/opsware/  
crypto/cgw0-LosAngeles/opswgw.pem
```

The lines that follow are from the properties file of the first Gateway in the San Jose Satellite:

```
opswgw.Gateway=SanJose1  
opswgw.Realm=SanJose  
opswgw.TunnelSrc=sanfran.myops.com:2001:100:0:/var/opt/opsware/  
crypto/SanJose1/opswgw.pem  
opswgw.TunnelSrc=losang.myops.com:2001:200:0:/var/opt/opsware/  
crypto/SanJose1/opswgw.pem
```

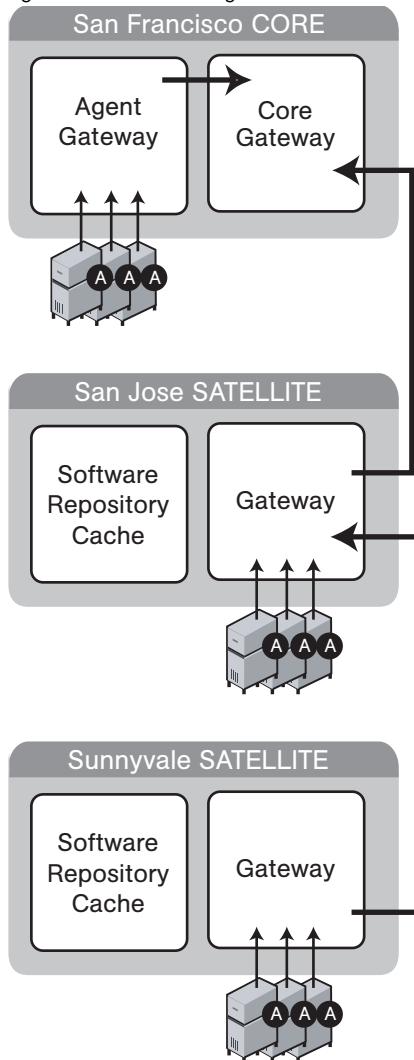
The next lines are from the properties file of the second Gateway in the San Jose Satellite:

```
opswgw.Gateway=SanJose2  
opswgw.Realm=SanJose  
opswgw.TunnelSrc=sanfran.myops.com:2001:100:0:/var/opt/opsware/  
crypto/SanJose2/opswgw.pem  
opswgw.TunnelSrc=losang.myops.com:2001:200:0:/var/opt/opsware/  
crypto/SanJose2/opswgw.pem
```


Cascading Satellites

Figure 9-4 is an example of cascading Satellites, a topology in which Satellite Gateways are connected in a chain. These Satellite Gateways must be in different realms. (For more information, see “Managing the Software Repository Cache” in the *Opsware® SAS Administration Guide*.)

Figure 9-4: Cascading Satellites With a Standalone Core



The following lines are from the core Gateway properties file of the San Francisco facility:

```
opswgw.Gateway=cgw0-SanFrancisco
opswgw.Realm=SanFrancisco
```

```
opswgw.TunnelDst=2001:/var/opt/opsware/crypto/cgw0-  
SanFrancisco/opswgw.pem
```

The lines that follow are from the Gateway properties file of the San Jose Satellite.

```
opswgw.Gateway=SanJose  
opswgw.Realm=SanJose  
opswgw.TunnelDst=2001:/var/opt/opsware/crypto/SanJose/  
opswgw.pem  
opswgw.TunnelSrc=sanfran.myops.com:2001:100:0:/var/opt/opsware/  
crypto/SanJose/opswgw.pem
```

The next lines are from the Gateway properties file of the Sunnyvale Satellite:

```
opswgw.Gateway=Sunnyvale  
opswgw.Realm=Sunnyvale  
opswgw.TunnelSrc=sanjose.myops.com:2001:100:256:/var/opt/  
opsware/crypto/Sunnyvale/opswgw.pem
```

Limiting Bandwidth

In Figure 9-4, suppose that the tunnel between Sunnyvale and San Jose shares a 512 kilobit/sec DSL connection with another application. Since this connection is relatively slow, you might want to limit the tunnel bandwidth to 256 kilobits/sec. To limit the bandwidth, you specify 256 for the fourth parameter of the `opswgw.TunnelSrc` property. (See the previous listing of the Sunnyvale properties file.) If you do not want to limit the tunnel bandwidth, set this parameter to 0. Note that the bandwidth parameter is not used to determine the cost of a route. (See “Configuring Routing (Cost)” on page 158.)

Satellite Installation

This section describes how to create a new Opware Satellite with the simple topology shown in Figure 9-1. This topology has the following characteristics:

- The Satellite contains one Opware Gateway and one Software Repository Cache, installed on the same server.
- The Satellite Gateway communicates with one core Gateway. No other Gateways communicate with the Satellite Gateway.

Required Information for Installing a Satellite

You will be prompted for the following information during the installation process:

- The password to decrypt cryptographic material. During the installation of the core, the Opware Installer prompts for this password.
- The IP address of the server running the core Gateway.
- The IP address of the server on which you will install the Satellite Gateway.
- The port of the tunnel destination of the core Gateway. (The default port is 2001.) The core Gateway listens on this port for a connection from the Satellite Gateway. In the core Gateway properties file, this port is the value of the `opswgw.TunnelDst` property. On the core Gateway server, the path of the properties file is as follows:

```
/etc/opt/opsware/opswgw-cgw0-<facility>/opswgw.properties
```

- The Opware user name (`admin`) and password of a user that belongs to the Administrators group.
- The name of the new Gateway in the Satellite. The new Gateway will be installed in the following directory:

```
/opt/opsware/opswgw/bin
```

- The name of the new realm to be serviced by the Gateway in the Satellite. Opware SAS uses the realm name and the IP address of a managed server to uniquely identify a managed server. The Opware Gateway Installer assigns the realm name to the new facility name of the Satellite. The core and Satellite facility names will be different. You may want to name the realm according to the physical location of the Satellite's data center, for example, the building, corporate site, or city. The Opware Command Center lists the facility names of the core and its Satellites.

Installing a Satellite

This section contains the step-by-step instructions for running the Opware Installer (`install_opsware.sh` script).

- 1** Obtain the Opware Server Automation System (SAS) installation media.
See “Installation Media for the Opware Installer” on page 97, including the recommendation, “Copying the DVD to a Local Disk.”
- 2** On the server where you will install the new Opware Satellite, mount the Satellite Base DVD or the Satellite Base Including OS Provisioning DVD or NFS-mount the directory that contains a copy of the DVD contents.



Whether you choose to install the Opware Satellite from the Satellite Base DVD or the Satellite Base Including OS Provisioning DVD depends on whether you install the OS Provisioning components in the satellite. See “Installation Media for the Opware Installer” on page 97 for information about each of the Opware SAS DVDs.

The Opware Installer must have read/write root access to the directories where it installs Opware components, even NFS-mounted network appliances.

3 In a terminal window log in as root.

4 Make the following directory:

```
mkdir -p /var/opt/opware/crypto/cadb/realm
```

5 Copy the database of cryptographic material and the Unix Tar file Gzipped from the core server to the Satellite server. On the core server, this database and the Unix Tar file Gzipped is in the following files:

```
/var/opt/opware/crypto/cadb/realm/opware-crypto.db.e
```

```
/var/opt/opware/crypto/cadb/realm/opware-crypto.tgz.e
```

The database of cryptographic material and the Unix Tar file Gzipped must be copied to the same directory and file names on the Satellite server. The directory and database and the Unix Tar file Gzipped need to be readable by the root user.

6 Change to the root directory:

```
cd /
```

7 Run the Opware Installer in interview mode by invoking it with no command-line options:

```
/opware_system/opware_installer/install_opware.sh
```

You must specify the full path to the script. The directory path shown in this step indicates that you copied an Opware SAS Satellite DVD (the Satellite Base DVD or the Satellite Base Including OS Provisioning DVD) to a local disk or a network share using the required directory structure.

8 At the interview mode prompt, select one of the following options:

- 1 - Simple Interview Mode
- 2 - Advanced Interview Mode

Option 1 is for using default values for many of the configuration parameters. Option 2 is for specifying all configuration parameters during the interview.

- 9** Respond to the interview prompts.

The `cgw_address` prompt is for the core Gateway, not the Satellite Gateway. For more information on the prompts, see Table 5-6 on page 93.

- 10** Decide if you want to finish the interview.

When you enter all of the required information, the Opware Installer displays this message:

```
All parameters have values. Do you wish to finish the
interview (y/n):
```

If you are satisfied with your answers, press `y`.

If you want to review or change your answers, press `n`. The installer displays the prompts again, showing in brackets `[]` the values that you previously entered.

- 11** Create the response file.

When you are finished with the interview, the installer prompts you for the name of the response file:

```
Name of response file to write
[/usr/tmp/oiresponse.satellite]
```

The response file is a text file that contains the answers you entered during the interview. You can enter the full path and name of the response file or accept the default. Note that the default file name corresponds to the type of installation.

- 12** The Opware Installer prompts you to indicate whether you want to continue the installation by using the response file:

```
Would you like to continue the installation using this
response file? (y/n):
```

If you are satisfied with the responses you entered in the interview and you are ready to install the Satellite now, enter `y` to continue. If you do not want to install the Satellite now, enter `n`.

- 13** If you entered `y` in the previous step, skip this step. If you entered `n` in the previous step, invoke the Opware Installer with the `-r` option to specify the response file created by the interview:

```
/opware_system/opware_installer/install_opware.sh -r
<full_path_to_response_file>
```

- 14** At the components prompt, select 1 to install the Opware Gateway. The components prompt follows:

```
Welcome to the Opware Installer.
Please select the components to install.
1 ( ) Opware Gateway (Interactive Install)
2 ( ) Software Repository Cache (wordcache)
3 ( ) OS Provisioning Boot Server
4 ( ) OS Provisioning Media Server
Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.
```

Selection: 1

Note that you must install the components in the order they are listed.

The selections for the OS Provisioning Boot Server and OS Provisioning Media Server only appear is you are running the installation from the Satellite Base Including OS Provisioning DVD.

- 15** Verify that the Opware Installer launches the Opware Gateway Installer, which displays the following banner:

```
*****
*
*                Opware Gateway Installer                *
*       Copyright (C) 2004-2006: Opware Inc.              *
*                support@opware.com                      *
*
*****
```

- 16** Verify that you have the necessary information for the Gateway, as described in “Required Information for Installing a Satellite” on page 162. The Opware Gateway Installer displays the following message:

For a new install please have the following information available before you begin:

- 1) Opware administrator username and password.
- 2) The Realm name this Gateway will service.
- 3) If the Realm is new what type will it be.
- 4) The unique Gateway name for this Gateway.

Are you ready to proceed? [y/n]

- 17** At the proceeding prompt, enter y. The Opware Gateway Installer displays the following lines:

```
=====
```

```
ISM install
=====
. . .
```

- 18** Enter the name of the realm for the Opsware Gateway you are installing. The prompt for the realm follows:

```
=====
Create/Verify Realm
=====
Enter the Gateway's Realm name:
You entered '<realm-name>', is this correct [y/n]
```

- 19** There are three ways for the installer to contact the Opsware core. At the prompt for the option number, enter 3. The installer displays the following lines:

```
I must now contact an Opsware Core to continue the
intallation...
There are three ways this can be done:
  1) Via an existing Gateway's ProxyPort
  2) Via direct connections (no NATs)
  3) Via a temporary (local) Gateway
Enter option number: 3
```

- 20** Enter the IP address of the server running the core Gateway at the following prompt:
Enter IP of a remote GW:

- 21** Enter the tunnel destination port of the core Gateway at the following prompt. The default port is 2001. (For more information, see “Required Information for Installing a Satellite” on page 162.)

```
Enter TunnelDst port of the remote GW: 2001
```

- 22** At the following prompt, enter y.

```
Is the tunnel listener at <ip-addr:port>
using SSL? [y/n] y
```

- 23** Enter the user name (admin) and password of an Opsware user that belongs to the Administrators group. The user name and password prompts follow.

```
=====
Connect to Opsware
=====

Log into Opsware as an administrator

Enter username:admin
Enter password:
```

- 24** Verify that the Opsware Gateway Installer displays the following lines:

```
=====
```

```
Checking time synchronization
=====

Gateway time looks good.
```

- 25** At the prompt that follows, enter 1 to create a new Satellite.

```
=====
Configure Realm
=====

The realm '<realm-name>' does not exist.  You have two
options:
  1) Create a new Satellite DC named '<realm-name>'.
  2) Add a new Realm, '<realm-name>', to an existing DC.
  3) Exit.
Enter option number: 1
```

- 26** At the following prompt, enter the name for the new Opware Gateway that you are installing.

```
=====
Gateway Configuration
=====

Enter the Gateway's name:
```

- 27** Verify that the Opware Gateway Installer opens the properties file in the vi text editor. The following lines are at the top of the properties file:

```
#####
#
# Opware Gateway Properties file for a SAT Gateway
#
#####
```

The full path name of the properties file follows:
/etc/opt/opware/opswgw-cgw0-<facility>/opswgw.properties

- 28** Opware Gateway Properties File: For the opswgw.GWAddress property, enter the IP address of the host on which you are installing this Gateway (that is, the host you are logged into now). Example:

```
opswgw.GWAddress=192.168.198.92
```

- 29** Opware Gateway Properties File: For the opswgw.TunnelSrc property, change the placeholder IP address of 10.0.0.11 to the IP address of the host running the core Gateway. The port following the IP address is the tunnel destination of the core Gateway. (The default port is 2001.) Example:


```
opswgw.TunnelSrc=192.168.165.242:2001:100:0:/var/opt/
opsware/crypto/<gateway-name>/opswgw.pem
```

- 30** Opsware Gateway Properties File: Because you are going to install a Software Repository Cache (wordcache) in a later step, verify that the following lines in the Opsware Gateway Properties file are not commented out:

```
opswgw.DoNotRouteService=theword:1003
opswgw.DoNotRouteService=127.0.0.1:1003
opswgw.HijackService=wordcache:1003
```

- 31** After you've finished editing the Opsware Gateway Properties in `vi`, save the file and exit `vi`.

- 32** Respond to the prompts that ask if you'd like to proceed. The Opsware Gateway Installer performs several more tasks and displays the following messages:

```
Gateway Crypto Generation
. . .
Wordcache Crypto Generation
. . .
Starting Opsware Gateway
. . .
Verify Gateway Startup
```

When it's finished, the Opsware Gateway Installer displays the following line:
Opsware Gateway Installed!

- 33** Invoke the Opsware Installer with the `-r` option to specify the response file created by the interview in step 11 on page 165:

```
/opsware_system/opsware_installer/install_opsware.sh -r
<full_path_to_response_file>
```

- 34** At the components prompt, select one or more components to install:

```
Welcome to the Opsware Installer.
Please select the components to install.
1 ( ) Software Repository Cache (wordcache)
2 ( ) OS Provisioning Boot Server
3 ( ) OS Provisioning Media Server
```

Enter a component number to toggle ('a' for all, 'n' for none).

When ready, press 'c' to continue, or 'q' to quit.

Selection:

You must install the components in the order they are listed. For example, you must install the Software Repository Cache before the OS Provisioning Boot Server.

The Software Repository Cache is required and must be installed on the same server as the Gateway.

The selections for the OS Provisioning Boot Server and OS Provisioning Media Server only appear if you are running the installation from the Satellite Base Including OS Provisioning DVD.

The OS Provisioning Boot Server and Media Server are required only if you want to use the Opware OS Provisioning feature in the Satellite. The OS Provisioning Boot Server and Media Server can reside on a different server than the Gateway and Software Repository Cache. (See step 35.)

If you are installing all of the components on the same server, then you may enter `a` for all. If you do not select `a`, then you must run the Opware Installer again (specifying the response file) and select the remaining components.

35 If you are installing the OS Provisioning components on a different server than the other Satellite components, follow the instructions in this step.

- Copy the database of cryptographic material and the Unix Tar file Gzipped from the server with the Satellite Gateway to the server that will run the OS Provisioning components. Here is the full path of to these files:

```
/var/opt/opware/crypto/cadb/realm/opware-crypto.db.e
```

```
/var/opt/opware/crypto/cadb/realm/opware-crypto.tgz.e
```

The database of cryptographic material and the Unix Tar file Gzipped must be copied to the same directory. The directory and files need to be readable by the root user.

- Copy the response file generated by the installer interview to the server that will run the OS Provisioning components.
- On the server that will run the OS Provisioning components, run the Opware Installer with the `-r` option, as shown in step 33. Select and install the remaining components from the menu shown in step 34.

Post-Installation Tasks for a Satellite

After you install a Satellite, perform the tasks listed in the following sections. For more information, see the Opware Satellite Administration section of the *Opware® SAS Administration Guide*.

Facility Permission Settings

The Opsware Gateway Installer assigns the realm name to the facility name of the Satellite. To access managed servers in the Satellite, an Opsware user must belong to a group that has the necessary permissions for the Satellite's facility. Until you set the facility permissions, Opsware users cannot view or modify the managed servers associated with the Satellite's facility. For example, you might set the permissions for the Satellite facility to Read & Write for the Advanced Users group, enabling members of this group to modify the servers managed by the Satellite.

For instructions, see "Setting the Facility Permissions of a User Group" in the *Opsware® SAS Configuration Guide*.

Checking the Satellite Gateway

To verify that the core Gateway is communicating with the Satellite Gateway, perform the following steps:

- 1** Log into the Opsware Command Center as a member of a users group that has the Manage Gateway permission.
- 2** From the navigation panel, select Administration ► Gateway.
- 3** Verify that the upper left corner of the Manage Gateway page displays a link for the new Satellite Gateway.

If the Manage Gateway page does not display the link for the Satellite, you might need to correct the properties file of the Satellite Gateway. The full path name of the properties file follows:

```
/etc/opt/opsware/opswgw-cgw0-<facility>/opswgw.properties
```

If you modify the properties file, you must restart the Satellite Gateway:

```
/etc/init.d/opsware-sas restart opswgw-cgw0
```

- 4** Log into the Opsware Command Center as a member of a users group that has the the Read (or Read & Write) permission on the Satellite's facility.
- 5** From the navigation panel, select Servers ► Manage Servers.
- 6** Verify that the Manage Server page displays the host name of the Satellite server.

Enabling the Display of Realm Information

By default, the Opsware Command Center does not display realm information, which is needed by users who manage Gateways and Software Repository Caches.

To enable access to the realm information, perform the following steps:

- 1** Log into the Opware Command Center as a user that belongs the Administrators group and to a group that has the Configure Opware permission.
- 2** From the navigation panel, click Administration ► System Configuration.
- 3** Select the Opware Command Center link.
- 4** In the System Configuration page, for the name `owm.features.Realms.allow`, type the value `true`.
- 5** Click **Save**.

DHCP Configuration for OS Provisioning

After you install the OS Provisioning Boot Server component, you must set up a DHCP server. For more information, see “DHCP Configuration for OS Provisioning” on page 117.

Chapter 10: What's Next

IN THIS CHAPTER

This section discusses the following topic:

- Configuration for Opsware SAS

Configuration for Opsware SAS

After you've completed the tasks in the preceding sections of this guide, the core components of Opsware SAS should be running and you should be able to log into the Opsware Command Center. Now, Opsware SAS is ready to be configured so that end users can start managing servers in the operational environment. The configuration tasks follow:

- **Configure e-mail alerts for Opsware SAS.**

The Opsware managed servers, the multimaster mesh, and the Opsware Code Deployment and Rollback feature can be configured to send e-mail alerts. Your e-mail administrator should set up the Opsware core and managed servers as sendmail clients. In the Opsware Command Center, you should configure the e-mail alerts before you install Agents on the managed servers. See the *Opsware® SAS Administration Guide* for information

- **Set up Opsware groups and users.**

To log on to the Opsware Command Center, you specify a user name and password. Each user belongs to a group, and each group has a set of permissions for specific Opsware features. When the user logs on to the Opsware Command Center, only those features permitted by the user's groups are displayed. Each group also has permissions to perform read and write operations on managed servers that are associated with customers or facilities. See the *Opsware® SAS Administration Guide* for information.

- **Create Opsware customers.**

When you ran the Opsware Installer for a standalone core, you specified a default customer. You may also create and assign new customers to the facility. See the *Opsware® SAS Policy Setter's Guide* for information.

- **Define you policies for Software Management.** See the *Opsware® SAS User's Guide: Application Automation* for information.

- **Install Opsware Agents on existing servers.**

After you install an Opsware Agent, the server may be managed with Opsware SAS. See the *Opsware® SAS User's Guide: Server Automation* for information.

- **Prepare Opsware SAS for OS Provisioning.**

When you provision (install) an OS on a server, Opsware SAS automatically installs an Agent. See the *Opsware® SAS Policy Setter's Guide* for information.

- **Prepare Opsware SAS for patch management.**

See the *Opsware® SAS User's Guide: Application Automation* for information.

- **Establish monitoring practices for Opsware SAS by performing the following tasks:**

- Run the Agent reachability tests in the Opsware Command Center. See the *Opsware® SAS User's Guide: Server Automation* for information.
- Run the diagnostic tests in the Opsware Command Center. See the *Opsware® SAS Administration Guide* for information.
- Review the Opsware SAS component log files. See the *Opsware® SAS Administration Guide* for information.

Chapter 11: Opsware SAS Uninstallation

IN THIS CHAPTER

This section discusses the following topics:

- Overview of Uninstalling Opsware SAS
- Procedures for Uninstalling Cores

Overview of Uninstalling Opsware SAS

You might need to uninstall an Opsware core in the following scenarios:

- You have an Opsware core in a lab setting before installing Opsware SAS in a production environment. You might want to uninstall the Opsware core after you finish testing it.
- You are consolidating facilities and want to uninstall an Opsware core in one facility in preparation to moving it to another facility.

Uninstalling the Model Repository permanently deletes all data in the database. But when you uninstall an Opsware core, you can choose to preserve the Opsware SAS data in the Model Repository database. If you choose to preserve this data, the Opsware Installer stops the uninstallation.

Stopping the uninstallation gives you the opportunity to back up the data in the Model Repository. After you begin the Model Repository uninstallation, the Opsware Installer will not preserve any data in the Model Repository.

You can also choose to preserve or remove all the packages stored on the Software Repository.

You can also choose to preserve the database of cryptographic material for the Opsware core. If you choose to preserve crypto, the database of cryptographic material will be saved; otherwise it will be deleted when the uninstallation finishes.



Before you uninstall an Opware core, Opware Inc. recommends that you back up the Oracle database running on the server where the Model Repository is installed. See your Oracle documentation for the steps required to back up an Oracle database.

Procedures for Uninstalling Cores

This section discusses the following topics:

- Uninstalling a Standalone Core
- Uninstalling One Core in a Multimaster Mesh
- Uninstalling an Entire Multimaster Mesh of Opware Cores
- Decommissioning a Facility in the Opware Command Center

Uninstalling a Standalone Core

Perform the following steps to uninstall a standalone core:

1 Before you uninstall the Opware core components from the servers running them, you should deactivate the servers in the Opware Command Center. Otherwise, if you try to re-install an Opware core component on one of the servers later, the installation will fail. (For more information, see “Deactivating a Server” in the *Opware® SAS User’s Guide: Server Automation*.)

2 Log in as root.

3 Change to the root directory:

```
cd /
```

4 Run the `uninstall_opware.sh` script:

```
/opware_system/opware_installer/uninstall_opware.sh -r  
<response-file>
```

5 At the components prompt, select one or more components to uninstall:

```
Welcome to the Opware Installer.  
Please select the components to uninstall.  
1 ( ) Opware Gateway  
2 ( ) OS Provisioning Build Manager  
3 ( ) OS Provisioning Media Server  
4 ( ) OS Provisioning Boot Server  
5 ( ) Opware Command Center (OCC)  
6 ( ) Opware Global Filesystem Server (OGFS)
```


- 7 () Software Repository (word)
- 8 () Command Engine (way)
- 9 () Data Access Engine (spin)
- 10 () Model Repository (truth)
- 11 () Oracle RDBMS

If the Opware Gateway does not run on a separate server, uninstall it last.

- 6** Remove the `/var/opt/opware/install_opware` directory.



If you indicated at the prompt that you want to preserve crypto (the database of cryptographic material), you should *not* delete the `/var/opt/opware/crypto` directory. Deleting this directory deletes the database of cryptographic material.

Uninstalling One Core in a Multimaster Mesh

When uninstalling a core from a multimaster mesh, you should not uninstall the source core unless you are planning to uninstall the entire mesh.

See “Uninstalling an Entire Multimaster Mesh of Opware Cores” on page 179 in this chapter for more information.

Perform the following steps to uninstall one core in a multimaster mesh:

- 1** Log into any Opware Command Center that is still online to perform the following tasks:
 1. Using the System Configuration feature, update the `listeners` configuration parameter by removing the entry for the core that is being uninstalled. Update the `listeners` parameter by selecting “Model Repository, Multimaster Component” in the System Configuration page.
 2. If a Data Access Engine that is being uninstalled is currently serving as the multimaster central role, a Data Access Engine in another core must be selected to serve as Multimaster Central.
See “Reassigning the Data Access Engine to a Secondary Role” in the *Opware[®] SAS Administration Guide*.
 3. Verify that all transactions have propagated to the other facilities, except for the facility that is being uninstalled.
See “Verifying Multimaster Transaction Traffic” on page 149.

- 2 Decommission the facility for the core you are uninstalling. See “Decommissioning a Facility in the Opware Command Center” on page 179.

- 3 Restart the Model Repository Multimaster Component in all cores except the core that is being uninstalled by entering the following command as root on the server running the engine:

```
/etc/init.d/opware-sas stop vaultdaemon  
  
/etc/init.d/opware-sas start vaultdaemon
```

- 4 Stop the Opware Command Center in the core that is being uninstalled by entering the following command as root:

```
/etc/init.d/opware-sas stop occ.server
```

- 5 In the core that is being uninstalled, stop all Data Access Engines.

Log in as root to the server where the Data Access Engine is running and enter the following command:

```
/etc/init.d/opware-sas stop spin
```

- 6 If the Opware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opware Command Center server.

- 7 Stop the Model Repository Multimaster Component in the core that is being uninstalled by entering the following command as root on the server running the engine:

```
/etc/init.d/opware-sas stop vaultdaemon
```

- 8 Restart the Data Access Engine that is serving as Multimaster Central by entering the following commands as root:

```
/etc/init.d/opware-sas stop spin  
  
/etc/init.d/opware-sas start spin
```

- 9 For the core that you are uninstalling, on each server running an Opware component, run the following script.

```
/opware_system/opware_installer/uninstall_opware.sh
```

Uninstall the components by following the instructions in step 4 through step 6 in the section “Uninstalling a Standalone Core.”

Uninstalling an Entire Multimaster Mesh of Opware Cores

Perform the steps in this procedure only when you want to uninstall all cores in a multimaster mesh:

- 1 Stop the Opware Command Center by logging on as root to the server where the Opware Command Center is running and enter the following command:

```
/etc/init.d/opware-sas stop occ.server
```

- 2 Stop the Data Access Engine.

Log in as root to the server where the Data Access Engine is running and enter the following command:

```
/etc/init.d/opware-sas stop spin
```

If the Opware Command Center and the Data Access Engine are installed on different servers, you must also run the `spin stop` command on the Opware Command Center server.

- 3 Stop the Model Repository Multimaster Component in all cores by logging in to the servers running the engines and entering the following command as root:

```
/etc/init.d/opware-sas stop vaultdaemon
```

- 4 In each core, uninstall the Opware components on the servers where they are installed.

```
/opware_system/opware_installer/uninstall_opware.sh
```

Follow the instructions in step 4 through step 6 in the section “Uninstalling a Standalone Core.”

Decommissioning a Facility in the Opware Command Center



Performing this procedure does not shut down or uninstall Opware SAS in a facility. Decommission facilities with care, because this task cannot be undone.

When you decommission a facility, the facility is still listed in the Opware Command Center, however, it is grayed out. After a short name is used, even if it is decommissioned, that name cannot be reused.

Perform the following steps to decommission a facility:

- 1** In the Opware Command Center, deactivate the server running the core of the facility that you wish to decommission. (For instructions, see "Deactivating a Server" in the *Opware® SAS User's Guide: Server Automation*.)
- 2** From the navigation panel, click Environment ► Facilities. The Facilities page appears.
- 3** Select the facility that you want to decommission.
- 4** On the Properties tab, note the answer to the following question:

Is this facility in use?

If the answer is No, the **Decommission** button is displayed.
- 5** Click **Decommission**.

Appendix A: TIBCO Rendezvous Configuration for Multimaster

IN THIS APPENDIX

This section discusses the following topics:

- TIBCO Rendezvous and Opsware SAS
- TIBCO Rendezvous Configuration

TIBCO Rendezvous and Opsware SAS

In a multimaster mesh, Opsware SAS uses the TIBCO Certified Messaging system to synchronize the Model Repositories in different facilities.



The Opsware Installer automatically installs and configures TIBCO Rendezvous. By default, the installer configures the Rendezvous neighbors in a star topology, in which the source core is at the center. Unless you want another configuration, no further action is required by you.

TIBCO Rendezvous Configuration

This section explains how to add TIBCO routers and neighbors. For more information, see the following TIBCO Rendezvous documentation:

- *TIBCO Rendezvous Installation Guide*
- *TIBCO Rendezvous Concepts*

Running the TIBCO Rendezvous Web Client

To run the TIBCO Rendezvous web client, enter the following URL in a web browser:

```
http://<hostname>:7580
```

The <hostname> is the IP address or fully-qualified host name of the server running the Model Repository Multimaster Component (vault). The TIBCO Rendezvous General Information page appears.

Adding a TIBCO Router

To add a TIBCO router, perform the following steps:

- 1** Run the TIBCO Rendezvous web client.
- 2** From the left navigation panel, click Routers under Configuration. The Routers Configuration page appears.
- 3** Make sure that your browser can resolve the host name so that the link in the Router Name field functions correctly.
- 4** In the Router Name field, enter a value. Usually, you enter the facility name for the router name.
- 5** Click **Add Router**. The new router appears in the table on the page.
- 6** In the Local Network column under Interfaces, click the number link for the router you just added. The Local Network Interfaces Configuration page appears.
- 7** Define a new network by entering the following data:
 1. In the Local Network Name field, enter the network name. In most cases, the network is given the same name as the facility name.
 2. In the Service field, set the service to 7500.
 3. Click **Add Local Network Interface**. The new local network appears in the table in the page.
- 8** Click the link for the new local network name. The Subject Configuration page appears.
- 9** In the Subject field, enter a greater-than symbol (>) and click **Import** and **Export**. (The greater-than symbol means “any.”) The greater-than symbol appears in the Import Subjects and Export Subjects tables in the page.
- 10** Repeat the previous steps for the other facilities in the multimaster mesh.

Adding a TIBCO Rendezvous Neighbor

To add a TIBCO Rendezvous neighbor, perform the following steps:

- 1** In the core Gateway properties file, add the following line:

```
opswgw.ForwardTCP=<port>:<remote_realm>:<remote_host>:7501
```

The <port> is derived from this formula: $10000 + \text{remote_facility_ID}$. The <remote_realm> is the realm name of the core Gateway in the remote facility. The <remote_host> is the IP address of the server running the Model Repository Multimaster Component (vault) in the remote facility. In the following example, the remote facility ID, is 667, the realm name is LIME, and the IP address of the Model Repository Multimaster Component is 192.168.165.98:

```
opswgw.ForwardTCP=10667:LIME:192.168.165.98:7501
```
- 2** Run the TIBCO Rendezvous web client.
- 3** From the left navigation panel, click Routers under Configuration. The Routers Configuration page appears.
- 4** In the Neighbor column of the table, click the number link for the router you added in the previous procedure. The Neighbor Interfaces Configuration page appears. You must define a neighbor for each facility in the multimaster mesh, except for the local facility.
- 5** In the Host field under the Remote Endpoint section, enter the host name of the server running the local core Gateway.
- 6** In the Port field under the Local Endpoint section, enter 7501.
- 7** In the Port field under the Remote Endpoint sections, set the port to the value derived from the following formula: $10000 + \text{remote_facility_ID}$.
- 8** In the Router Name field under the Remote Endpoint section, enter the router name for the other facility.
- 9** For the Connection Type, select Normal Connection.
- 10** Click **Add Neighbor Interface**. The Local and Remote endpoints are added to the table in the page.

Verifying TIBCO Rendezvous Configuration

To see if the neighbor has connections to a facility, perform the following steps:

- 1** Run the TIBCO Rendezvous web client.

- 2 Click Connected Neighbors in the left navigation panel. For each neighbor you defined for this facility, you should see links for the rvr interface.

Appendix B: Opsware Gateway Properties File

IN THIS APPENDIX

This section discusses the following topics:

- Syntax of the Opsware Gateway Properties File
- Options for the opswgw Command

Syntax of the Opsware Gateway Properties File

An Opsware Gateway properties file can have the following entries:

`opswgw.Gateway=name`

(Required) Set the name of the Opsware Gateway. This name must be unique in a Gateway network.

`opswgw.Realm=realm`

(Required) All Opsware Gateways operate in a named realm. A realm is an abstract name given to the collection of servers which are serviced by the Gateways in the realm. Realms can support an IP address space which may overlap with another realm. Realms are also used to define bandwidth utilization constraints on Opsware SAS functions in that realm.

`opswgw.Root=true | false`

Indicates that this Gateway should act as a root of the Gateway network. All Gateways in a root realm must be root Gateways. The default is false.

`opswgw.Daemon=true | false`

Daemonize the process. The default is false.

`opswgw.Watchdog=true | false`

Start an internal watchdog process to restart the Gateway in case a failure or a signal. A SIGTERM sent to the watchdog will stop the watchdog and Gateway processes. The default is false.

`opswgw.HardExitTimeout=seconds`

The number of seconds the main thread will wait (after a restart or exit request) for internal threads and queues to quiesce before a hard exit is performed.

`opswgw.LogLevel=INFO | DEBUG | TRACE`

Set the logging level. The DEBUG and TRACE produce a lot of output which will only be relevant to developers. The default is INFO.

`opswgw.LogFile=file`

The basename of the log file.

`opswgw.LogNum=num`

The number of rolling log files to keep.

`opswgw.LogSize=size`

The size in bytes of each log file.

`opswgw.TunnelDst=[lip1:]lport1[:crypto1],...`

Start up a tunnel destination listener. The tunnel listener can listen on a list of ports (a comma-separated list with no spaces.) If the port is prefixed with an IP, then the listener will only bind to that IP address. Examples: 2001, 10.0.0.2:2001, 2001:/var/foo.pem, 10.0.0.2:2001:/var/foo.pem

```
opswgw.TunnelSrc=rhost1:rport1:cost1:bw1[:crypto1],...
```

Create a tunnel between this Gateway and the Gateway listening at `rhost1:rport1`. The link `cost1` and link bandwidth `bw1` must be set. The cost is a 32bit unsigned int, and bandwidth is in Kbits/sec (K=1024bits). (Additional tunnels are separated by commas.) Examples: `gw.foo.com:2001:1:0`,
`gw.bar.com:2001:10:256:/var/foo.pem`

```
opswgw.TunnelTCPBuffer=bytes
```

Set the size TCP send and recv buffer to `bytes`. The system's OS must be configured to handle this value. View the Gateway's log file to see if the value given here will work on the current system.

```
opswgw.ValidatePeerCN=true | false
```

Indicates whether the peer CN be validated. The peer needs to be turned off during the installation of an untrusted Gateway. The default is true.

```
opswgw.ProxyPort=[lip1:]lport1,[lip2:]lport2,...
```

The SSL proxy listen port. If more than one proxy listen port is needed, add more using a comma separated list.

```
opswgw.ForwardTCP=[lip1:]lport1:realm1:rhost1:rport1,...
```

Create a static TCP port forward. Forward the local port `lport` to the remote service `rhost:rport`, which is in `realm`. A blank `realm` (e.g., `lport::rhost:rport`) means route to the root realm.

```
opswgw.ForwardUDP=[lip1:]lport1:realm1:rhost1:rport1,...
```

Create a static UDP port forward. Forward local port `lport` to remote service `rhost:rport`, which is in `realm`. If `realm` is blank (e.g., `lport::rhost:rport`) it means route to the root realm. (Warning: Some UDP services, such as DHCP, cannot be proxied in this manner.)

`opswgw.GWAddress=lhost`

Set the local host address (IP or name) that this Gateway uses to tell other components how to contact it. This value is used by the core to discover new core-side Gateways. It is also used to communicate the active list of Gateways that are servicing a realm to proxy clients (such as Agents) via the X-OPSW-GWLIST mime header.

`opswgw.IdentPort=[lip:]lport`

Start up an ident service listening on local port `lport`.

`opswgw.FinalizeTCPPortMap=true|false`

If true, remove the TCP source port from the ident port map immediately before the socket is closed. If false, the mapping persists until the port is reused. Warning: Only use false if you know what you are doing. The default is true.

`opswgw.FinalizeUDPPortMap=true|false`

If true, remove the UDP source port from the ident port map immediately before the socket is closed. If false, the mapping persists until the port is reused. Warning: Only use false if you know what you are doing. The default is true.

`opswgw.AdminPort=[lip:]lport[:crypto1]`

Start up an administration interface listening on local port `lport`, which is optionally bound to the local IP `lip`. If `crypto` is desired, then include a crypto specification file name.

`opswgw.ConnectionLimit=int`

The soft memory tuning limit of maximum number of connections.

`opswgw.OpenTimeout=seconds`

Only wait this many seconds for a remote `CONNECT` call to establish a remote connection.

`opswgw.ConnectTimeout=seconds`

Only wait this many seconds for the `connect()` to complete. If a timeout occurs, then an HTTP 503 message is returned to the client (via the ingress Gateway). The client will get this message if the `ConnectTimeout` plus the Gateway mesh transit delay is less than the `OpenTimeout`.

`opswgw.ReorderTimeout=seconds`

In the event of out-of-order messages (for a TCP flow), limit the amount of time to wait for messages (needed for reassembly) to arrive.

`opswgw.QueueWaitTimeout=seconds`

Maximum time that a tunnel message can wait at the head of an internal routing queue (while waiting for a tunnel to be restored).

`opswgw.LsaPublishRate=seconds`

Send the Link State Advertisements (LSAs) every X seconds.

`opswgw.LsaExtendRate=count`

Send an extended LSA for every count number of normal LSAs. Example: If `LsaPublishRate` is 10.0 seconds and `LsaExtendRate` is 30, then every 30 LSAs (about every 300 seconds) an extended LSA is published.

`opswgw.LsaTTLMultiple=float`

Set the TTL for LSAs to this number multiplied by the `LsaPublishRate`. Example: If `LsaPublishRate` is 10 seconds and `LsaTTLMultiple` is 3 then, the TTL for LSAs published by this Gateway is set to 30 seconds.

`opswgw.LsaExtendTTLMultiple=float`

Set the TTL for extended LSAs to this number multiplied by the `LsaPublishRate` and the `LsaExtendRate`. Example: If the `LsaPublishRate` is 15 seconds and the `LsaExtendRate` is 30 and the `LsaExtendTTLMultiple` is 8, then the TTL for extended LSA information is 3600 seconds (because $15 * 30 * 8 = 3600$). One function of the in-memory database of the extended LSA information is to form the `X-OPSW-GWLIST` MIME header.

`opswgw.MaxRouteAge=seconds`

Discard the routes from the routing table that have not been refreshed within this number of seconds.

`opswgw.TunnelTimeoutMultiple=float`

This number, multiplied by the `LsaPublishRate`, gives the maximum time that a tunnel can be idle before it is garbage collected.

`opswgw.DoNotRouteService=host1:port1,host2:port2,...`

If a local client creates a proxy connection to `host:port`, then do not route the message; service it locally. This is used to handle certain services locally in the Gateway's current realm.

`opswgw.ForceRouteService=
host1:port1:realm1,host2:port2:realm2,...`

If local client creates a proxy connection to `host:port`, then force the message to route to realm.

`opswgw.HijackService=host1:port1,host2:port2,...`

If the local Gateway sees a connection to `host:port` via a tunnel, and the source realm is different than the local realm, then service the connection. Otherwise, let the message continue to its destination. This feature is useful for implementing transparent caches.

`opswgw.EgressFilter=tcp:dsthost1:dstport1:srchost1:srcrealm1,...`

If the local Gateway sees a `tcp` connection attempt to `dsthost:dstport` from `srchost1:srcrealm1`, then allow the connection. The implied default is to deny all connections. If you want to allow all traffic, then specify `*:*:*:*:*`. Watch out for shell quoting. It is common for an egress filter to only allow connections from the root realm. This can be expressed by leaving the `srcrealm` blank. Example:

`tcp:10.0.0.5:22:172.16.0.5:` would allow `tcp` connections to 10.0.0.5, port 22, from 172.16.0.5 in a root realm.

```
opswgw.IngressMap=ip1:name, ip2:name, . . .
```

When sending an open message (and the `srcip` is in the ingress map), append (as metadata) the `ip:name` mapping to the open message. This allows a remote egress filter to use the name as the `srchost` instead of the `ip`. This feature supports the addition of a server to a farm without the need to add the server to many `EgressFilter` entries.

```
opswgw.LoadBalanceRule=  
tcp:thost:tport:mode:rhost1:rport1:rhost2:rport2, . . .
```

When receiving an open connection message for `thost:tport`, load balance the connection over real hosts `rhost1:rport1`, `rhost2:rport2` etc. The load balance strategy is defined by `mode`. There is currently only one mode: `STICKY`. This mode does sticky load balancing based on a hash of the source realm and `ip`. Remember to add an egress filter for `thost:tport`. You do not need to add egress filters for the targets. Load balancing is only for `tcp` connections.

```
opswgw.LoadBalanceRetryWindow=seconds
```

If an error occurs when using a load balanced target (e.g., `rhost1:rport1` above) then the target is marked `in-error`. This parameter controls how many seconds a Gateway will wait until it re-tries the target. If the target is missing (i.e., an `RST` is received upon the connection request) the load balancer will silently try to find a good target.

```
opswgw.MinIdleTime=seconds
```

The minimum number of seconds a connection can be idle, during an overload condition, before it will be considered for reaping.

```
opswgw.GCOverloadTrigger=float
```

The fraction of `SoftConnectionLimit` at which to start overload protection measures. When the number of open connections hits this overload trigger point, the overload protection kicks in, reaping the most idle connections over `MinIdleTime`. Overload protection quits when the connection count falls below the overload trigger point.

`opswgw.GCCloseOverload=true | false`

When a client tries to open a connection after the `ConnectionLimit` has been reached, this property tells the Gateway what to do with the new connection. A value of `true` causes the Gateway to close the new connection. A value of `false` causes the Gateway to park the new connection in the kernel's backlog and to service it once the overload condition subsides. The proper setting is application dependent. The default is `false`.

`opswgw.VerifyRate=seconds`

When a connection stops moving data for this number of seconds, a connection verify message is sent to the remote Gateway to check that the connection is still open on its end. This check is repeated periodically and indefinitely when the timeout has expired.

`opswgw.OutputQueueSize=slots`

The size of the tunnel output queues. These queues store messages destined for remote Gateways. Each remote Gateway has an output queue.

`opswgw.DefaultChunkSize=bytes`

The default (maximum) IO chunk size when encapsulating a TCP stream. This default is only used on links with no bandwidth constraint.

`opswgw.LinkSaturationTime=seconds`

On links with a bandwidth constraint, the chunk size (see `DefaultChunkSize`) is computed based on two parameters. The first is the link's bandwidth constraint. The second is the amount of time that the bandwidth shaper should utilize the full, real, bandwidth on the link. This parameter controls the duty cycle of the bandwidth shaper. Smaller values give a smoother bandwidth control at the cost of more overhead, because each smaller IO chunk has a header.

`opswgw.MaxQueueIdleTime=seconds`

The maximum time to keep an idle output queue before garbage collection removes it.

`opswgw.TunnelPreLoad=slots`

The maximum number of output queue slots to use before waiting for the first Ack message. This allows for pipelining in Long Fat Pipes. This value is reduced geometrically to one as the number of queue slots diminish.

`opswgw.BandwidthAveWindow=samples`

The maximum number of IO rate samples for the bandwidth estimation moving window. The samples in this window are averaged to provide a low pass estimate of the bandwidth in use by a tunnel. This estimate has high frequency components due to the sharp edge of the filter window.

`opswgw.BandwidthFilterPole=float`

The pole of a discrete-time first-order smoothing filter used to remove the high frequency components of the moving window estimator. Set the value to 0.0 to turn off this filter.

`opswgw.StyleSheet=URL`

Add a stylesheet link to URL when rendering the admin UI. This is useful for embedding the admin UI in another web-based UI. In addition to using this property to control the default stylesheet, a dynamic stylesheet override is supported by adding the variable `StyleSheet=;url;/style.css` to the admin UI URL.

`opswgw.PropertiesCache=file`

Link cost and bandwidth can be controlled via parameter-modify messages over the tunnel connections. These real-time adjustments are made to the running process and written to a parameter cache which will override the properties file or command line arguments.

Options for the opswgw Command

All of the properties in the preceding section can be specified as options for the `opswgw` command. For example, the `opswgw.Gateway=foo` entry in the properties file is equivalent to the following command-line option:

```
/opt/opsware/opswgw/bin/opswgw --Gateway foo
```

Command-line arguments override corresponding entries in the properties file. In addition to the entries listed in the preceding section, the `opswgw` command can specify a properties file as follows:

```
/opt/opsware/opswgw/bin/opswgw --PropertiesFile file
```

Index

A

- accessing, realm information 171
- adding
 - core to multimaster mesh 139
 - TIBCO Rendezvous neighbor 183
 - TIBCO router 182
- Agent. See Opsware Agent.
- agent-server architecture 29
- agent-server architecture, Opsware SAS 18
- associating, customers with a new facility 149

B

- bandwidth 162
- Boot Server
 - defined 29, 32
- Build Agent, defined 30, 35
- Build Manager
 - defined 29, 32

C

- cascading Satellites 161
- checking
 - Satellite Gateway 171
- checklists 66
- Command Engine
 - defined 29
 - scripts 32
- command line options 97
- Components of Multimaster Installations 134
- configuration
 - Gateway for Satellite 154
 - Opsware SAS 173
 - TIBCO Rendezvous 181
- configuration tracking 60
- configuring
 - DHCP server for OS Provisioning 120
 - existing DHCP server 122
 - MS Windows DHCP Server 126
 - Opsware and MS Windows DHCP servers 127

- conventions used in the guide 13
- cost, definition of 158
- creating, silent installable version of IE 6.0 130

D

- Data Access Engine
 - defined 29, 32
- deactivating, facilities 179
- DHCP
 - configuration for OS provisioning 117
 - defined 117
 - dhcpd.conf 118
 - dhcpcdtool 118, 120
 - existing 52
 - existing server 122
 - MS Windows 126, 127
 - Opsware DHCP Server 117, 120
 - proxy 56, 118
 - starting and stopping 122
- DMZ 57
- DNS 55, 129
- dormant, Opsware Agents 34
- duplex setting 53
- DVD 97

F

- facilities
 - associating, customers 149
 - deactivating 179
 - definition of 64
 - multimaster 142
 - names 141
 - network requirements 53
 - prompts 85
 - realm names 163
 - scaling 46
 - setting, permissions 171
- failover 159
- firewall 53, 54

G

Gateway properties file 183, 185

H

host names resolution 55, 129, 136, 152

I

IDE disks 52

Inbound, Model Repository Multimaster
Component 33

installations

checklist 66

converting, from standalone to multimaster
136

hardware requirements 42

installation media 97

Opware Satellite 151, 162

process flow 64

standalone 101

types 63

installing, Windows Agent Deployment Helper
112

instances 47

interview, overview 99

L

load balancer 47

local networks 117

locale 62, 87

log files 99

logging in

OCC 107

M

managing, DHCP server 122

Media Server

defined 29, 32

Model Repository

defined 30, 33

password prompts 79

prompts 76

Model Repository Multimaster Component

defined 30, 33

Inbound 33

Outbound 33

model-based approach

servers, affects on 19

multimaster

adding, core 139

converting, standalone to 136

installation 63

overview of support in Opware SAS 21

post-installation tasks 149

prerequisites 135

uninstalling, core 177

uninstalling, multimaster mesh 179

verifying, transaction traffic 149

with Satellites 157

N

NAS Duplex Data Gathering diagnostic 116

NAS Topology Data Gathering diagnostic 116

networks

DHCP network configuration tool 119

local 117

network requirements within a facility 53

OS provisioning network requirements 56,
129

remote 118

Satellites 153

NFS 50, 53, 153

NIS 53

NTP 61, 136

O

open firewall ports

between core servers and managed servers
55

on core servers 53

OS provisioning components for 54

open ports for OS provisioning 129

open ports for Satellite 152

open TCP ports 53

operating systems

creating, silent installable version of IE 6.0
130

prerequisites, Windows NT 4.0 and Windows
2000 for 130

requirements for Linux 51

requirements for Solaris 49

Opware Agent

defined 30

dormant 34

Installer 34

overview 18, 33

Opware Agent Installer 34

- Opware Command Center
 - defined 30, 34
 - logging in 107
 - multimaster mesh 135
 - password 108
 - password for logging in to OCC. 84
 - Opware component password prompts 83
 - Opware components
 - additional instances 47
 - overview 31
 - Opware core
 - adding, to a multimaster mesh 139
 - checklist for installation 68
 - converting, standalone to multimaster 136
 - installation process flow 64
 - installation requirements 70
 - uninstallation prompts 96
 - uninstalling 176
 - Opware Gateway
 - checking, Satellite Gateway 171
 - configuration for Satellite 154
 - defined 30, 36
 - Gateway properties file, syntax of 185
 - multiple 159
 - opswgw command, options of 194
 - prompts 93
 - Opware Global File System
 - defined 37
 - Opware Global File System, prompts 94
 - Opware guides
 - contents 11
 - conventions used 13
 - documentation set 15
 - icons in guide, explained 14
 - Opware Installer
 - command line options 98
 - command line syntax 97
 - installation media 97
 - Installer interview 75
 - interview 99
 - logs 99
 - Opware SAS
 - agent-server architecture 18, 29
 - components 31
 - components overview 29
 - configuration 173
 - documentation set 15
 - model-based approach, affecting servers 19
 - related documentation 15
 - supported operating systems 39, 40, 42
 - uninstalling 175
 - Opware Satellite
 - accessing, realm information 171
 - cascading 161
 - checking, Satellite Gateway 171
 - definition 63
 - installation, overview 151
 - installing 162
 - linked to cores 63
 - multimaster mesh 157
 - multiple Gateways 159
 - required open ports 152
 - requirements 152
 - setting, facility permissions 171
 - standalone core 154
 - topologies 154
 - Opware System
 - scaling 46
 - opswgw 194
 - Oracle
 - client 77
 - home 77
 - password 79
 - remote database 77
 - SID 77
 - supported versions 40
 - tnsnames.ora 76, 77, 105, 136, 148
 - OS Build Agent. *See* Build Agent.
 - OS provisioning
 - DHCP configuration 117
 - DHCP network configuration tool 119
 - DHCP proxying 56
 - network requirements 56, 129
 - open firewall ports 54
 - open ports 129
 - prompts 88
 - Outbound, Model Repository Multimaster Component 33
- P**
- password, logging into OCC for 108
 - patch management
 - prerequisites for Windows NT 4.0 and Windows 2000 130
 - prompts 88
 - requirements 57
 - ports
 - open firewall ports 55
 - open firewall pots for OS provisioning 54
 - open ports, Satellite for 152
 - open TCP ports 53

- post-installation multimaster tasks 149
- prerequisites
 - installing, standalone core 102
 - multimaster installation for 135
 - patch management on Windows NT 4.0 and Windows 2000 130
- prompts
 - facility 85
 - Model Repository 76
 - Model Repository, password prompts 79
 - Opware component password prompts 83
 - Opware Gateway 93
 - Opware Global File System 94
 - OS provisioning 88
 - patch management 88
 - uninstallation 96
- Python 32

R

- realm 155, 156, 159, 161, 163
- reconciling 35
- remote networks 118
- requirements
 - checklist for core installation 70
 - component name resolution 55
 - for Linux 51
 - for patch management 57
 - for Satellite 152
 - for Solaris 49
 - hardware requirements for Opware core servers 42
 - network requirements within a facility 53
 - network, OS provisioning for 129
 - See also networks.
- running, TIBCO Rendezvous Web Client 181
- rurd 135, 184

S

- Satellite. See Opware Satellite.
- scaling
 - multiple facilities 46
- scripts
 - Command Engine 32
- server management
 - model-based approach 19
 - multiple facilities, in 19
- servers
 - hardware requirements for Opware core servers 42

- model-based approach 19
- references for managing DHCP 122
 - See also open firewall ports.
 - See also server management.
- setting, facility permissions 171
- Software Repository
 - defined 30, 35
- Software Repository Cache 154, 156
 - defined 30, 36
 - entries required 152
 - network storage 153
- Software Repository Multimaster Component
 - defined 30
- Software Repository Replicator
 - defined 30, 35
- Software Repository, Multimaster Component
 - defined 36
- source core, definition of 133
- standalone installation 63
 - converting, multimaster to 136
 - overview 101
 - uninstalling 176
 - with Satellite 154
- starting, DHCP server 122
- stopping, DHCP server 122
- supported operating systems
 - for managed servers 40
 - for Opware core components 39
 - for SAS Client 42

T

- target core, definition of 133
- TIBCO Rendezvous 135
 - adding, neighbor 183
 - adding, router 182
 - running 181
 - verifying, configuration 183
- time zone 61
- tools, DHCP network configuration tool 119
- transaction, definition of 149
- tunnel, definition of 154

U

- uninstalling
 - a core in a multimaster mesh 177
 - entire multimaster mesh 179
 - overview 175
 - prompts 96
 - standalone core 176

UTC 61, 153
UTF-8 62

V

verifying
 multimaster transaction traffic 149
 TIBCO Rendezvous configuration 183

W

Web Services Data Access Engine
 defined 30, 36

