



Planning Deployments for Opsware[®] SAS 5.2

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

Copyright © 2000-2005 Opsware Inc. All Rights Reserved.

Opsware Inc. Unpublished Confidential Information.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

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

Opsware, Opsware Command Center, Model Repository, Data Access Engine, Web Services Data Access Engine, Software Repository, Command Engine, Opsware Agent, Model Repository Multimaster Component, and Code Deployment & Rollback are trademarks and service marks of Opsware 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.opsware.com/support/opensourcedoc.pdf>.

Table of Contents

| | |
|--|-----------|
| Preface | v |
| <hr/> | |
| About this Guide | v |
| Contents of this Guide | v |
| About Opsware Documentation | vi |
| Conventions in This Guide | vi |
| Icons in This Guide | vi |
| Guides in the Documentation Set and Who Should Read Them | vii |
| Contacting Opsware, Inc. | viii |
| Chapter 1: Introduction to Opsware SAS | 1 |
| <hr/> | |
| Overview of Opsware SAS | 1 |
| Types of Opsware Users | 3 |
| Opsware SAS Features | 4 |

| | |
|---|-----------|
| Software Provisioning | 6 |
| Operating System Provisioning | 8 |
| Patch Management | 9 |
| Code Deployment & Rollback | 9 |
| Configuration Tracking | 10 |
| Script Execution | 10 |
| Data Center Intelligence Reporting | 11 |
| Discovery and Agent Deployment..... | 13 |
| Server Explorer..... | 14 |
| Server Compliance..... | 14 |
| Visual Packager | 15 |
| Application Configuration Management..... | 15 |
| Global Shell | 16 |
| Business Goals | 16 |
| Chapter 2: Opware SAS Architecture | 27 |
| Types of Opware SAS Installations | 27 |
| Opware SAS Components | 28 |

| | |
|---|------------|
| Boot Server | .31 |
| Build Manager | .31 |
| Command Engine | .31 |
| Data Access Engine | .31 |
| Media Server | .31 |
| Model Repository | .32 |
| Model Repository Multimaster Component | .32 |
| Opware Agents | .32 |
| Dormant Opware Agents | .33 |
| Opware Command Center | .33 |
| OS Build Agent | .34 |
| Software Repository | .34 |
| Software Repository Replicator | .34 |
| Software Repository Cache | .35 |
| Software Repository Multimaster Component | .35 |
| Web Services Data Access Engine | .35 |
| Opware Gateway | .35 |
| Global File System Server | .36 |
| Opware SAS Topologies | .36 |
| Benefits of a Multimaster Mesh | .36 |
| Example Multimaster Topologies | .36 |
| Benefits of Opware Satellites | .38 |
| Example Satellite Topologies | .38 |
| Chapter 3: Supported Operating Systems and Hardware Requirements | 45 |
| Supported Operating Systems | 45 |

| | |
|---|---------------|
| Supported Operating Systems for Opsware Core Servers | 45 |
| Supported Operating Systems for Opsware Agents, Opsware Command Center, and OCC Client. | 46 |
| Hardware Requirements for Opsware Core Servers | 48 |
| CPU Requirements. | 48 |
| Memory Requirements | 48 |
| Disk Space Requirements. | 48 |
| Opsware Core Scalability for Performance. | 49 |
| Factors Affecting Performance | 51 |
| Scaling Opsware SAS With a Multimaster Mesh | 51 |
| Additional Instances of Opsware Components and Load Balancing | 52 |
| Appendix A: Glossary | 53 |

Preface

Welcome to Opsware Server Automation System (SAS) – an enterprise-class software solution that enables customers to get all the benefits of Opsware, Inc. 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.

About this Guide

Contents of this Guide

This guide contains the following chapters and appendix:

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

Chapter 2: Opsware SAS Architecture: provides an overview of Opsware SAS architecture, how Opsware SAS components interact, and a description of the types of installations – standalone core, multimaster core, and Opsware Satellites.

Chapter 3: Supported Operating Systems and Hardware Requirements: provides a guide to determining how many servers you will need to run the Opsware core based on the metrics in your facility and how to correctly distribute the components for the core across the servers.

Appendix A: Glossary: defines terms that are unique to Opsware SAS.

About Opsware Documentation





Conventions in This Guide

This guide uses the following typographical and formatting conventions.

| NOTATION | DESCRIPTION |
|------------------------|--|
| <code>Courier</code> | Identifies text of displayed messages and other output from Opsware programs or tools. |
| Courier Bold | Identifies user-entered text (commands or information). |
| <i>Courier Italics</i> | Identifies variable user-entered text on the command line or within example files. |

Icons in This Guide

This guide uses the following iconographic conventions.

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

Guides in the Documentation Set and Who Should Read Them

- The *Opware[®] SAS 5.2 User's Guide* is intended to be read by the system administrator who is responsible for performing the day-to-day functions of managing servers, provisioning operating systems, uploading packages, setting up the Software Tree and node hierarchies, attaching software applications and installing them on servers, managing patches, reconciling servers with software, creating and executing scripts, tracking configuration, and deploying and rolling back code and content. It also documents the day-to-day functions of managing servers, such as server compliance and auditing, software packaging, application configuration, agent deployment, and global shell remote data center management.
- The *Opware[®] SAS 5.2 Administration Guide* is intended to be read by Opware administrators who will be responsible for setting up accounts for users, creating user groups and additional Opware administrators, assigning permissions for different levels of operation and access, adding customers and facilities, and monitoring and diagnosing the health of the Opware SAS components.
- The *Opware[®] SAS 5.2 Deployment and Installation Guide* is intended to be used by system administrators who are responsible for the installation of Opware SAS in a facility. It documents how to run the Opware Installer and how to configure each of the components.
- The *Planning Deployments for Opware[®] SAS 5.2* is intended to be used by advanced system administrators who will be responsible for planning all facets of an Opware SAS installation and deployment. It documents all the main features of Opware SAS and scopes out the planning tasks necessary to successfully deploy Opware SAS. Sections include: planning the Opware SAS design for a core, types of installations, and discusses business goals that can be achieved using the software. It also includes information on system sizing, checklists, and best practices.
- The *Opware[®] SAS 5.2 Configuration Guide* is intended to be used by system administrators who are responsible for all facets of configuring the Opware Command Center. It documents how to set up users and groups, configure Opware server management, and setting up the main Opware Command Center features, such as patch management, configuration tracking, software repository replicator setup, code deployment, as well as OS and software provisioning.

Contacting Opware, Inc.

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

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

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

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

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

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

The Opware Customer Support email address and phone number follow:

- [support@opware.com/](mailto:support@opware.com)
- +1 (877) 677-9273

Chapter 1: Introduction to Opsware SAS

IN THIS CHAPTER

This chapter discusses the following topics:

- Overview of Opsware SAS
- Opsware SAS Features
- Business Goals

Overview of Opsware SAS

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

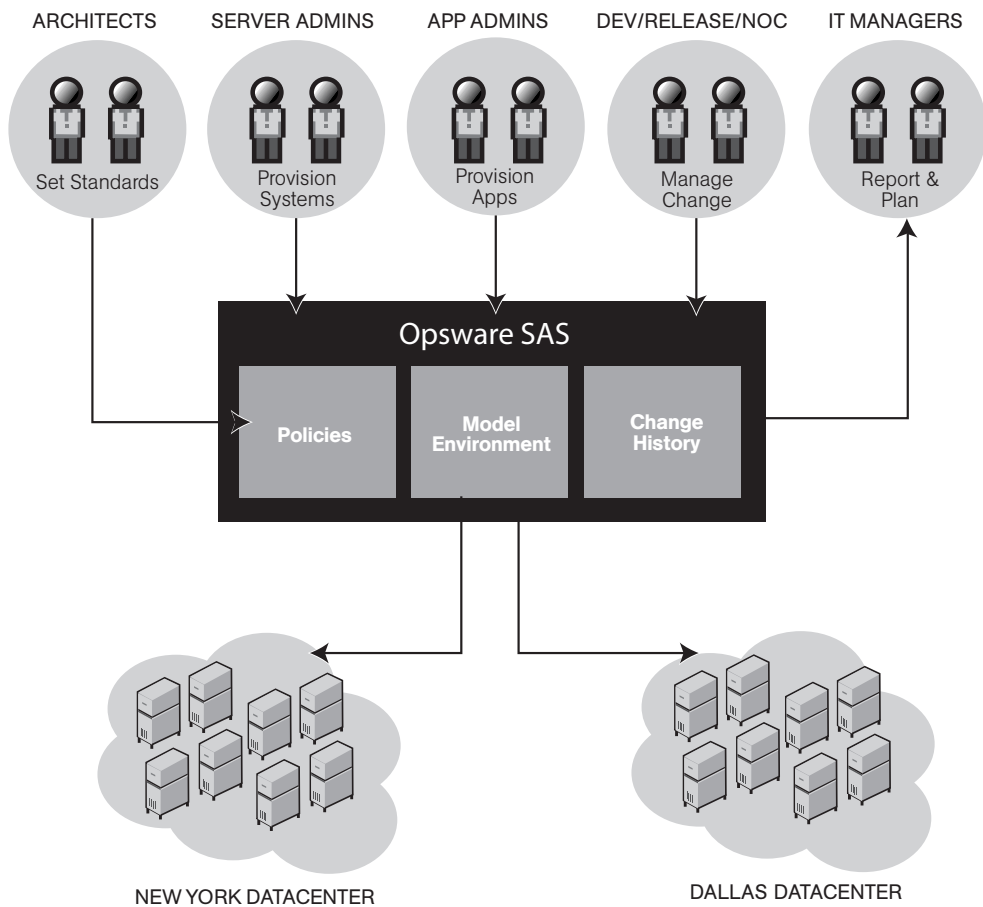
Opsware SAS does not just automate your operations, it also allows you to make changes more safely and consistently, because you can model and validate changes before you actually commit the changes to a server. Opsware SAS also helps ensure that modifications to your servers work on your first time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

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

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

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

Figure 1-1: Overview of Opsware SAS Features



Types of Opware Users

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

Table 1-1: Types of Opware Users

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

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

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

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

Opsware SAS Features

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

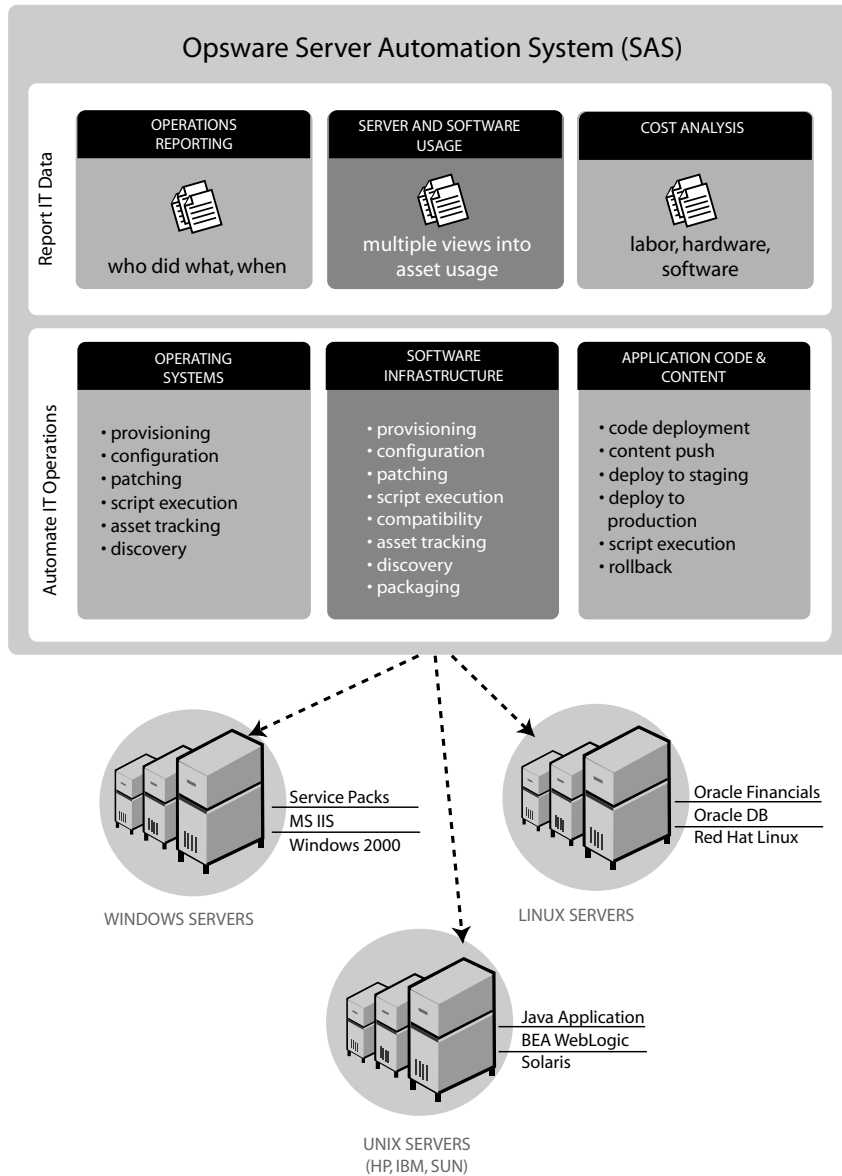
The features are designed to replace ad hoc, error-prone, manual processes. For example, by using the OS Provisioning feature, users can set standards for different types of servers and automatically provision the servers, saving time and ensuring that operating system builds are consistent. By using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

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

- Software Provisioning
- Operating System Provisioning
- Patch Management
- Code Deployment & Rollback
- Configuration Tracking
- Script Execution
- Data Center Intelligence Reporting
- Discovery and Agent Deployment

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

Figure 1-2: Opware SAS Features



Software Provisioning

The Software Provisioning feature provides a systematic way to install, configure, and remove packaged software across Windows, Unix, and Linux servers distributed across different data centers. Opware SAS's unique model-based approach enables many different teams, such as the system administration team, the database team, and the application development team, to manage the same set of servers. Each of these teams has a common view of the environment.

The Software Provisioning feature leverages Opware SAS's model-based approach, which provides the following unique capabilities and benefits:

- **Detailed information about the latest system state and configurations**

The Software Provisioning feature automatically creates and updates two lists: the list of software that users indicate should be installed on a server and the list of software that is actually installed on a server. By maintaining this detailed model of the server's current state, Opware SAS helps keep different IT groups managing the same server in sync and ensures that all groups making server changes are working with the same knowledge of the current state of the environment.

Using this model, Opware SAS enables multiple groups to manage the same server without stepping over each other's changes. An accurate model of the software installed on a server, granular role-based access control, a unified audit trail, and the ability to roll back changes, all contribute to Opware SAS's ability to coordinate the activities of many different administrators managing the same server.

- **Integration with other automation functions**

The Software Provisioning feature is fully integrated with other Opware SAS features, enabling software provisioning to be performed automatically with other tasks, such as operating system provisioning. Because software provisioning shares the same environment model as the other functions, the state of the environment is always known. This means that different groups, such as OS administrators, application administrators, security administrators, and others, can work together and communicate more effectively.

- **Simulation of software installation and removal**

Opware SAS's provisioning engine simulates installation and uninstallation actions before it applies changes to production servers. Users can view the list of software packages to be added or removed before they authorize Opware SAS to execute the

change. This ensures that all changes are pre-tested and validated before propagating changes to the production environment.

- **An up-to-date model of the actual server environment**

Opware SAS regularly refreshes its view of what is installed on a server, including both hardware and software. This real-time understanding of server state and configurations ensures that administrators provision the right software to the right servers at the right time. It also ensures that dependencies and prerequisites are checked and installed as needed.

- **Sophisticated role-based access control**

Opware SAS enforces a security policy that allows only authorized users to install or remove particular types of software on a particular server. For example, companies can define an access control rule that permits only DBAs to add or remove database software from a server.

- **A unified audit trail**

Opware SAS maintains a comprehensive audit trail of the software that Opware users install, configure, and remove from a server. When combined with the additional events that Opware SAS tracks – including configuration updates, business application pushes and rollbacks, hardware upgrades, and executed scripts – organizations gain a complete view of server activity over time.

- **The ability to roll back to a last known good state**

The Software Provisioning feature allows users to back out of software provisioning operations. In the event an upgrade or installation goes awry, administrators can back out the change to return to the last known good state.

- **Ability to store powerful name-value pairs**

Opware SAS helps organizations increase software package re-use by enabling administrators to install the same software package on different servers. Server-specific configuration values are fetched from Opware SAS (or calculated based on those values).

Operating System Provisioning

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

Benefits of the OS Provisioning feature include the following items:

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

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

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

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

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

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

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

- Preparing the hardware for OS installation
- Installing a base operating system and default OS configuration
- Applying the latest set of OS patches, the exact list depends on the applications that are going to run on the server

- Installing system agents and utilities such as SSH, PC Anywhere, backup agents, monitoring agents, or anti-virus software
- Installing widely-shared system software such as Java Virtual Machines
- Executing pre-installation or post-installation scripts that configure the system with values such as a root password

Patch Management

The Patch Management feature provides two features critical to patch management: the ability to react quickly to newly-discovered threats and the degree of control required to ensure that a new patch has been properly tested and installed in a uniform way.

Opware SAS has a deep understanding of native patch formats and structure. System administrators upload patches directly into Opware SAS, which understands and respects the structure of those patches in their native forms. It treats Solaris patch clusters, for example, differently from Windows Hotfixes or AIX APARs. Native patch support greatly increases both the flexibility and reliability of patch installation.

The Patch Management feature provides the following functionality:

- Scalable, cross platform patch deployment
- Reduced risk throughout automated patch rollback
- A central, shared patch repository to improve access
- Secure access control
- The ability to install patches on one server, or simultaneously on many servers
- The ability to schedule automated future installation (for example, to take advantage of maintenance windows)
- The inclusion of patches in the template for an operating system, so all newly provisioned servers receive the most up-to-date set of recommended patches

Code Deployment & Rollback

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

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

Configuration Tracking

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

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

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

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

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

Script Execution

The Script Execution feature enables you to share and run ad-hoc or custom scripts across an entire farm of Opware-managed servers. By executing scripts with Opware SAS instead of manually, administrators benefit by using the following features:

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

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

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

Data Center Intelligence Reporting

Every change made to your managed servers is recorded in Opsware SAS's Model Repository. The Model Repository maintains precise information about the state and configuration of every server under your management.

You can now take advantage of this information through Opsware SAS's Data Center Intelligence Reporting (DCI) component. The DCI provides accurate, detailed, and up-to-date information about your operational environment. The DCI provides a new level of visibility into your operational environment that can help organizations make better decisions.

DCI reporting provides the following features and benefits:

- **Exact information about the latest system state and configurations**

DCI reports display the most accurate and up-to-date information available, even during periods of frequent and substantial change. This level of accuracy reduces your risk of making the wrong decisions because of old data.

- **Visibility across the data center environment**

Opsware SAS provides a comprehensive view across all operating systems and locations, allowing IT managers to generate on-demand snapshots driven from a single, high-quality data source. The ad-hoc capability allows you to view a variety of report types, filter by specific criteria, and display summary graphics or list views. In addition, a set of Quick Reports are pre-designed for one-click access to real-time information from the Reports Home page.

- **Accurate and detailed change history information**

When a server's performance suddenly degrades, the best way to diagnose the cause is to learn the changes made to the server and who made the changes. Often, talking with the people who made the changes can help you understand the cause of the performance degradation.

In most facilities, however, it's often difficult, if not impossible, to find out a server's exact change history, since records are not accurately kept. But Opsware SAS maintains a detailed record of each change: who made the change, what was the nature of the change, and when it occurred. This record is presented in a comprehensive series of reports; these reports can significantly reduce the time and effort in debugging server and software problems.

- **A comprehensive set of patch reports**

One of the most time-consuming aspects of patching servers is identifying the vulnerable servers. Data collection for this task typically involves manually logging in to each server to see if it contains a particular version of software, what patches are already installed on the server, and what patches are *not* installed on the server.

Opware SAS helps administrators avoid this up-front effort by offering a comprehensive set of patch management reports.

- **The ability to extend the DCI reports**

You can also create new reports or modify the reports that ship with Opware SAS. Opware SAS provides the database necessary for creating reports.

The Reports Home page checks for any new custom reports that you create, and presents them on the Reports Home page for easy access to all users. These reports are created by using the readily available Crystal Reports Designer 9.

New reports can be extended to integrate with your own data sources (databases, spreadsheets, XML, and so forth), creating a powerful tool for more advanced data intelligence.

See the *Opware SAS DCI 1.6 Administrator's Guide* for information about how to set up the DCI Reporting component.

See the online Data Center Intelligence help and tutorial documentation for information about how to use and run the reports.



The Opware Data Center Intelligence Reporting component is an optional component. By default, it is not installed with Opware SAS. If this reporting component is not available for your organization, contact your Opware Support Representative for information about how to obtain it so that you can generate reports. The DCI component must be installed and running in order to access the online documentation.

Discovery and Agent Deployment

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

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

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

Server Explorer

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

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

- Create a server snapshot, perform a server audit, audit application configurations, create a package, and open a remote terminal session on a remote server.
- Browse a server's file system, registry, hardware inventory, software and patch lists, and services.
- Browse Opsware information such as properties, configurable applications, and even server history.
- Drag-and-drop files between your desktop and servers.

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

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

Server Compliance

The Opsware Server Compliance feature enables you to keep managed servers up-to-date by comparing them to a known working server. Server Compliance is an auditing feature intended to help you investigate and identify servers that are not performing well. You can use these audit results to troubleshoot and fix servers that are malfunctioning.

Using Opsware Server Compliance, you can perform the following tasks:

- Compare servers or snapshots to reference servers or snapshots.
- Create compliance audits for repeated use.
- Associate audits with individual servers or dynamic server groups.
- Remediate problems at multiple levels, including files, directories, patches, registry keys, and packages.

Visual Packager

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

Create Package is intended for system administrators who manage the software and configuration for groups of servers in Opware SAS.

You can selectively package server objects according to the operating system of the servers that you want to distribute the package to. Create Package supports Unix and Windows operating systems by allowing packages to contain the following objects:

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

Application Configuration Management

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

Using ACM, you can perform the following tasks:

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

Global Shell

The Opware Global Shell feature is intended for the Opware end user (the system administrator) who prefers to manage servers by using a command-line interface. Global Shell enables the system administrator to remotely perform the following tasks:

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

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

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

Business Goals

The following tables list types of datacenter business problems in these categories:

- Efficiency, Cost, and Productivity
- Consistency and Quality
- Visibility
- Security
- Downtime
- Risk

Table 1-2: IT Efficiency, Cost, and Productivity Issues

| BUSINESS PROBLEM: IT EFFICIENCY, COST, & PRODUCTIVITY | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|--|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| Computing resources are consumed by updating all files instead of only those that changed. | X | | | | | | | | | | | | | |
| It takes too long to find information for software planning and license tracking. | | | X | | | | | | | | | | | |
| Administrator accountability and problem solving is hampered by a lack of change history reporting across all servers and software. | | | X | | | | | | | | | | | |
| I need access to database views for integration with my corporate reporting tools. | | | X | | | | | | | | | | | |
| Remote server management is difficult, preventing me from accessing servers in all our data centers. | | | | X | | | | | | | | | | |
| Real-time secure replication of server and software information to all data centers is crucial. | | | | X | | | | | | | | | | |
| I need to replicate software between data centers and store it locally. | | | | X | | | | | | | | | | |
| If a conflict occurs in the synchronization of data between my data centers, I need to resolve it not just quickly, but also remotely. | | | | X | | | | | | | | | | |
| Manual Windows provisioning takes too long. I need a network-based remote unattended solution. | | | | | | | | | X | | | | | |

Table 1-2: IT Efficiency, Cost, and Productivity Issues

| BUSINESS PROBLEM: IT EFFICIENCY, COST, & PRODUCTIVITY | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|--|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| I want to automatically deploy applications like SQL Server and Norton Antivirus to many servers simultaneously. | | | | | | | | | X | | | | | |
| I need to schedule OS, application, Hotfix and Service Pack installation to coincide with my change windows. | | | | | | | | | X | | | | | |
| When executing VB scripts and batch files on multiple servers, I want to receive consolidated result output and a detailed audit trail. | | | | | | | | | X | | | | | |
| The code deployment process is complex and performed by numerous people, leading to inconsistencies in the application environment. It's worse if we need to rollback to a previous version. | X | | | | | | | | | | | | | |
| I want to provision servers on all platforms from Windows to Solaris to Linux using a single tool. | | | | | X | | | X | | | | | | |
| I don't want to have to perform complicated rewiring or network setup just to provision operating systems on my servers. | | | | | X | | | | | | | | | |
| I need to provision operating systems to servers via the network or CD. | | | | | X | | | | | | | | | |
| Our environment has older and newer hardware and I need a tool that can provision my legacy servers, not just the newer ones. | | | | | X | | | X | | | | | | |
| Configuring network settings automatically would allow us to eliminate the manual steps required to hand the server off to the application team. | | | | | X | | | | | | | | | |

Table 1-2: IT Efficiency, Cost, and Productivity Issues

| BUSINESS PROBLEM: IT EFFICIENCY, COST, & PRODUCTIVITY | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|---|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| I need to repurpose servers to take advantage of existing hardware. | | | | | X | | | | | | | | | |
| A secure, task-based user interface would enable our administrators to provision servers remotely. | | | | | X | | | X | | | | | | |
| I want to write and execute scripts in languages I already know like Unix, Linux, and Visual Basic. | | | | | | | X | | | | | | | |
| I want to tailor the behavior of my scripts so that script values can be associated with individual servers, server groups, and particular software. | | | | | | | X | | | | | | | |
| We have a heterogeneous server environment running everything from Windows to HP-UX. I want to implement a system to manage everything. | | | | | | | | X | | | | | | |
| I want to provision software across hundreds of servers simultaneously. | | | | | | | | X | | | | | | |
| It's time-consuming to reformat software in a proprietary packing format when we provision software. We want keep it in its native format. | | | | | | | | X | | | | | | |
| I want to easily check what patches are installed on Windows, Linux, Solaris, AIX, and HP-UX servers. | | | | | | X | | | | | | | | |
| When applying patches, I need to tailor each patch with scripts that cover pre- or post-installation or uninstallation tasks, including stopping and starting services, changing configurations, and testing the patches. | | | | | | X | | | | | | | | |

Table 1-3: IT Visibility Issues

| BUSINESS PROBLEM: IT VISIBILITY | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|--|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| An audit trail is not available when code and content are updated; therefore, I do not know the “who, what, when, and where” of application updates and rollbacks. | X | | | | | | | | | | | | | |
| I can't detect when configuration changes occurred in our environment; therefore I can't perform proactive problem prevention. | | X | | | | | | | | | | | | |
| Server security audit trails are not easily available. | | X | | | | | | | | | | | | |
| Problem diagnosis takes too long. | | X | | | | | | | | | | | | |
| I do not have a view into cross-platform IT assets. | | | X | | | | | | | | | | | |
| It takes too long to gather the information needed when budgeting for and upgrading hardware. | | | X | | | | | | | | | | | |
| I need to view data by server business attributes such as server usage, lifecycle stage, business unit, facility, and location. | | | X | | | | | | | | | | | |
| Patching levels across platforms are not easily obtainable, making it difficult to quickly assess the vulnerabilities of specific servers. | | | X | | | | | | | | | | | |
| The possibility of targeting the wrong servers exists when planning important changes. | | | X | | | | | | | | | | | |

Table 1-3: IT Visibility Issues

| BUSINESS PROBLEM: IT VISIBILITY | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|--|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| I need to see a real-time view of server consolidations, new application deployments, and patch rollouts. | | | X | | | | | | | | | | | |
| I need a way to report on server security by quickly analyzing large numbers of servers for missing Hotfixes and Service Packs. | | | | | | | | | X | | | | | |
| Keeping track of changes to critical files and configuration objects like Registry Keys, the COM+ object database and the IIS Metabase is needed to provide visibility into the latest state of each of our servers. | | | | | | | | | X | | | | | |
| I need to know when one-off manual changes are made to our servers, and I need the ability to roll the changes back if I don't like the results. | | | | | | | | | X | | | | | |
| Patch compliance needs to be audited and reported on. | | | | | | X | | | | | | | | |

Table 1-4: IT Risk Issues

| BUSINESS PROBLEM: IT RISK | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|--|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| The inability to verify changes from deploying code before the changes are applied to the live production environment is a problem. | X | | | | | | | | | | | | | |
| It takes too long to back up software configuration before making changes. | | X | | | | | | | | | | | | |
| The possibility of targeting the wrong servers exists when planning important changes. | | | X | | | | | | | | | | | |
| Determining installation order of Hotfixes and Service packs and when to reboot is a chore, especially when doing it one server at a time. | | | | | | | | | X | | | | | |
| Too many errors related to installing and upgrading software are possible. I need to see the effect that changes will have before making them. | | | | | | | | X | | | | | | |
| I need to verify every server that requires patching is identified and patched. | | | | | | X | | | | | | | | |
| I want to scan our Windows servers to compare their patches with Microsoft's database of available (mssecure.xml). | | | | | | X | | | | | | | | |
| If a patch proves to be problematic, I need to roll that patch back. | | | | | | X | | | | | | | | |

Table 1-5: IT Disaster Recovery

| | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|--|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| BUSINESS PROBLEM: IT DISASTER RECOVERY | | | | | | | | | | | | | | |
| Server state information becomes out-of-date as soon as manual changes are made, lengthening the time to disaster recovery and restoration of previously-working configurations. | | X | | | | | | | | | | | | |
| It is difficult to track, back up, or restore critical configuration data across all major platforms. | | X | | | | | | | | | | | | |
| Configuration information is not being duplicated between multiple data centers. | | X | | X | | | | | | | | | | |
| Business continuity and disaster recovery is essential to my continuity of operations plan. | | | | X | | | | | | | | | | |
| I need a disaster recovery plan that includes software automatically replicated in each data center. | | | | X | | | | X | | | | | | |

Table 1-6: IT Security Issues

| | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|---|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| I need to prevent unauthorized users from pushing changes to servers. | X | | | | | | | | | | | | X | |
| I need role-based access control to manage our servers. | | | | | | | | | | | | | X | |
| Scripts – private and shared – need to be managed so that only authorized users can publish and execute them. | | | | | | | X | | | | | | | |

BUSINESS PROBLEM: IT SECURITY

Table 1-7: IT Downtime Issues

| | CDR | CONFIG TRACKING | DCI REPORTING | MULTIMASTER | OS PROV | PATCH MGMT | DSE | SOFTWARE PROV | WINDOWS SERVER MGMT | SHELL AND OGFS | SERVER COMPLIANCE | APP CONFIG | SERVER GROUPS | VISUAL PACKAGER |
|---|-----|-----------------|---------------|-------------|---------|------------|-----|---------------|---------------------|----------------|-------------------|------------|---------------|-----------------|
| BUSINESS PROBLEM: IT DOWNTIME | | | | | | | | | | | | | | |
| Downtime and slow time-to-repair occurs when our system needs to be restored to its prior state. | X | | | | | | | | | | | | | |
| The inability to quickly rollback to a previous working state after server downtime is a problem. | X | X | | | | | | | | | | | | |

Chapter 2: Opware SAS Architecture

IN THIS CHAPTER

This chapter discusses the following topics:

- Types of Opware SAS Installations
- Opware SAS Components
- Opware SAS Topologies

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.

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 Opsware core or Satellite is associated with a specific facility.

Opsware SAS Components

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

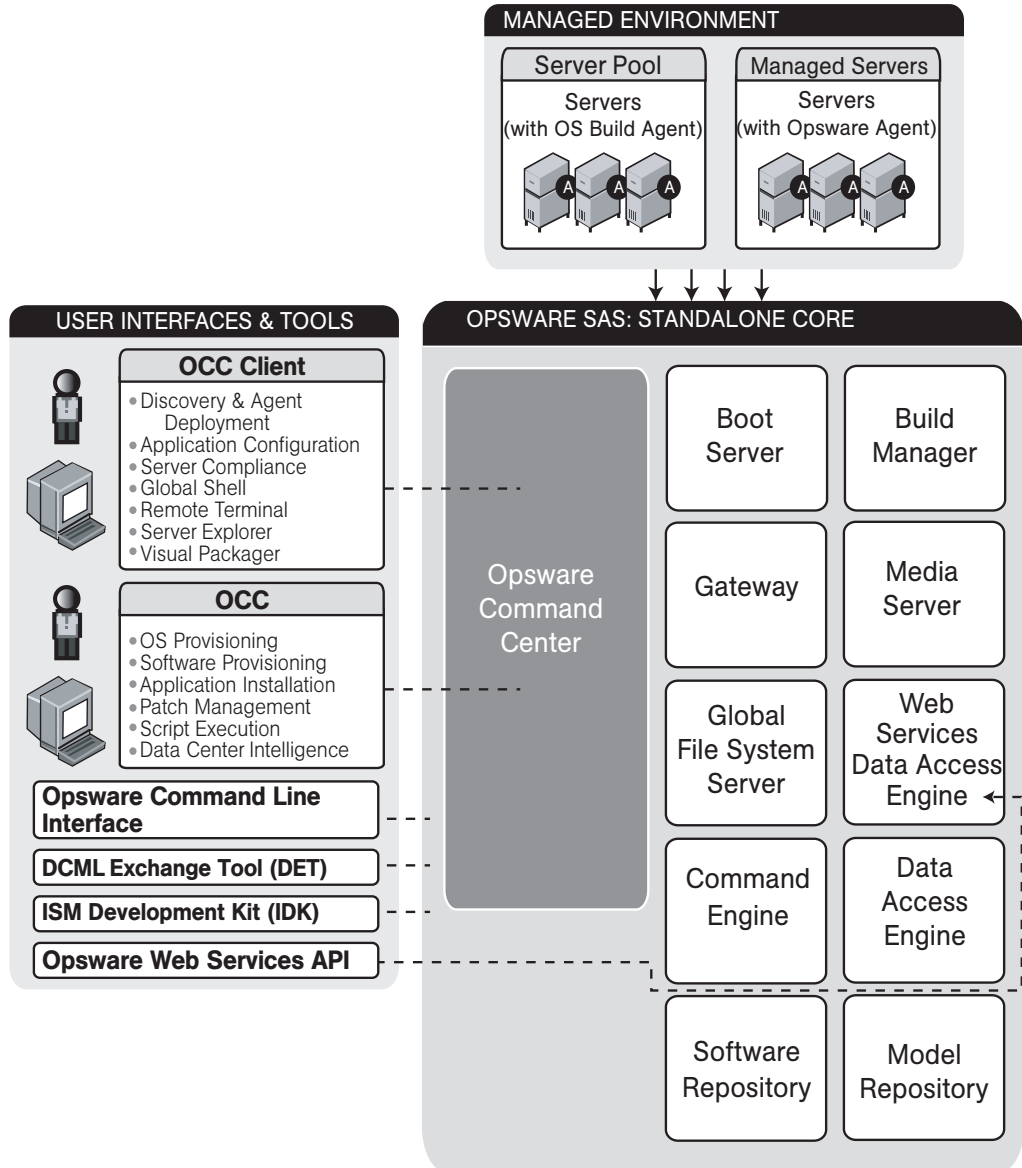
The sections that follow describe the components of Opsware SAS:

- **Boot Server:** Part of the OS Provisioning feature, supports network booting of Sun and x86 systems.
- **Build Manager:** Facilitates communication between components for OS provisioning.
- **Command Engine:** A system for running distributed programs across many servers.
- **Data Access Engine:** An XML-RPC interface to the Model Repository.
- **Media Server:** Provides network access to vendor-supplied media used during OS provisioning.
- **Model Repository:** Opsware SAS's 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.
- **Opsware Agents:** An intelligent agent that runs on each server that Opsware SAS manages.
- **Opsware Command Center:** A user interface to Opsware SAS.
- **OS Build Agent:** Responsible for registering a bare metal server with Opsware SAS and guiding the OS installation process.
- **Software Repository:** The central repository for all software that Opsware SAS manages.

- **Software Repository Replicator:** 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:** 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:** Contains local copies in the Opsware Satellite of the the Software Repository of the core (or another Satellite).
- **Web Services Data Access Engine:** Provides increased performance from the Model Repository to other Opsware SAS components.
- **Opsware Gateway:** Provides network connectivity to Opsware cores and Satellites.
- **Global File System Server:** Dynamically constructs the Opsware 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 2-1: 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 Boot 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 make Remote Procedure Calls (RPC) on 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 Opware Agent might use global Opware SAS services (such as the Model Repository and Software Repository) in order to fulfill the request.

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 Opware Agent is idle unless Opware SAS is trying to perform some change on the server. In addition, each Opware 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 Opware Agents

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

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

Opware Command Center

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

The Opware 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 Opware 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) through to the point at which 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 5.2 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 Opsware 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, if a Solaris package that resides on Software Repository (A) is needed for installation in a second facility that contains Software Repository (B) that 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 Opsware SAS components like the Opsware Command Center. It provides increased performance to other Opsware SAS components.

Opsware Gateway

The Opsware Gateway allows an Opsware 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 Opsware 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 Opsware Gateways service the managed servers contained within an Opsware realm. In Opsware SAS, a realm is a routable IP address space, which is serviced by one or more gateways. All managed servers that connect to an Opsware core via a gateway are identified as being in that gateway's realm.

Global File System Server

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

Opware SAS Topologies

Opware SAS requires at least one Opware 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, Opware Satellites, or a combination of both. For more information, see the *Opware® SAS 5.2 Deployment and Installation Guide* and the *Opware® SAS 5.2 Administration Guide*.

Benefits of a 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 Opware 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 Opware 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 Opware SAS running in other facilities.
- **Performance Scalability:** An Opware 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 2-2 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.

Figure 2-2: Multimaster Mesh With Two Cores

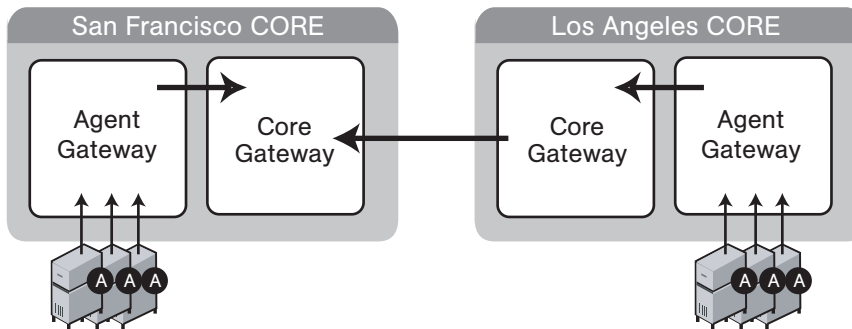
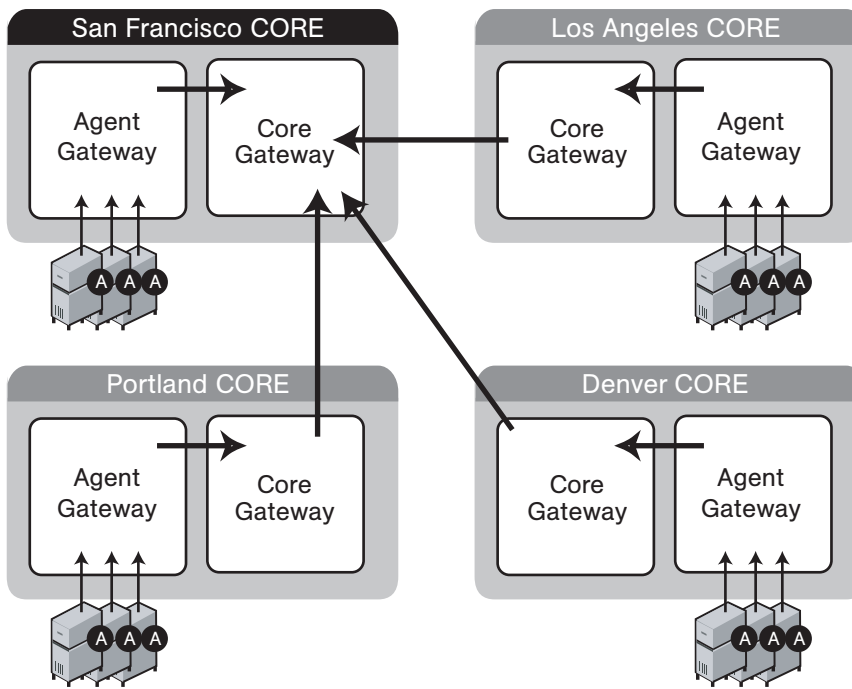


Figure 2-3 shows a multimaster mesh with several cores. This topology is in a star format with the San Francisco core is at the center of the mesh. By default, the Opsware Installer configures a multimaster mesh with a star topology.

Figure 2-3: 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 2-4 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 (...). 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.

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 2-4: Satellite With Standalone Core

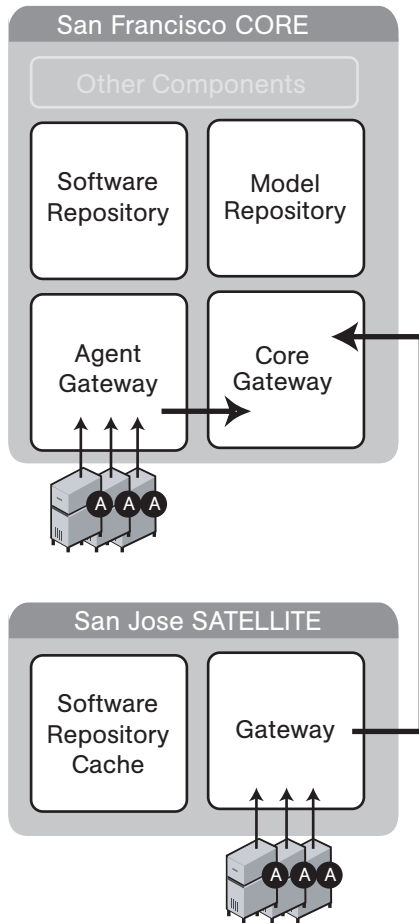


Figure 2-5 shows two Satellites linked to a standalone core. In this example, San Francisco, Sunnyvale, and San Jose are separate facilities. San Francisco is the large primary facility. Sunnyvale and San Jose are small remote facilities.

Figure 2-5: Two Satellites With a Standalone Core

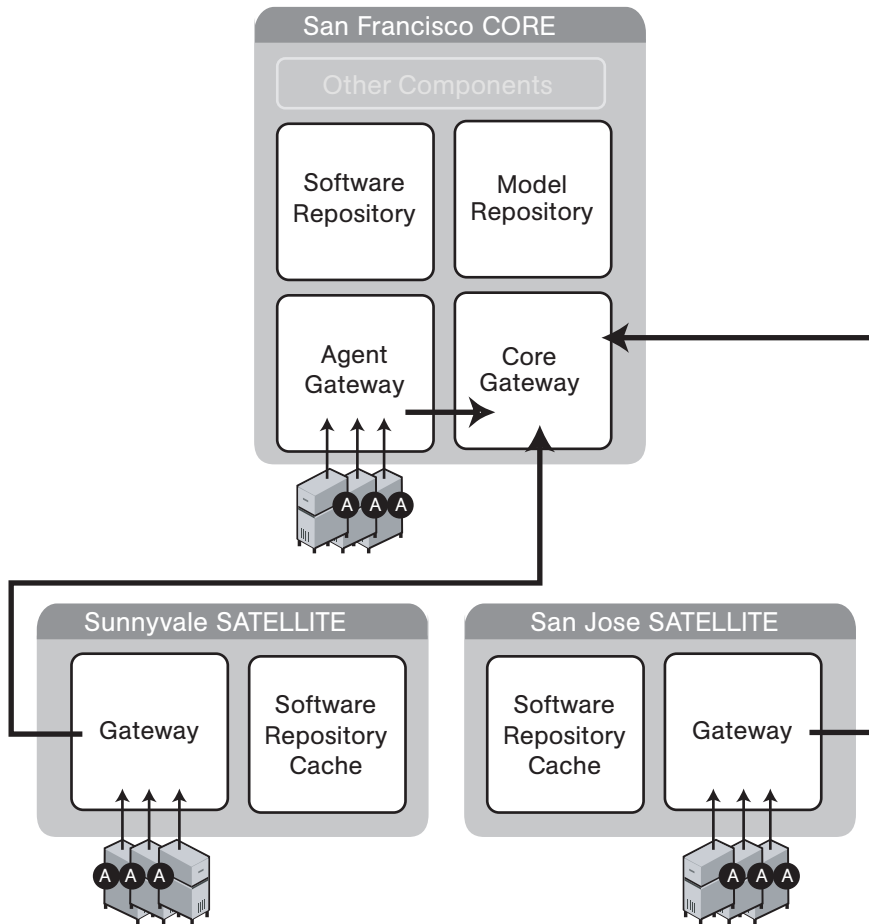


Figure 2-6 shows cascading Satellites, a topology in which Satellite Gateways are connected in a chain. This topology enables you to create a hierarchy of Software Repository Caches. The Satellite Gateways in this topology must belong to different realms. To install a package on a managed server in the 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 5.2 Administration Guide*.

Figure 2-6: Cascading Satellites With a Standalone Core

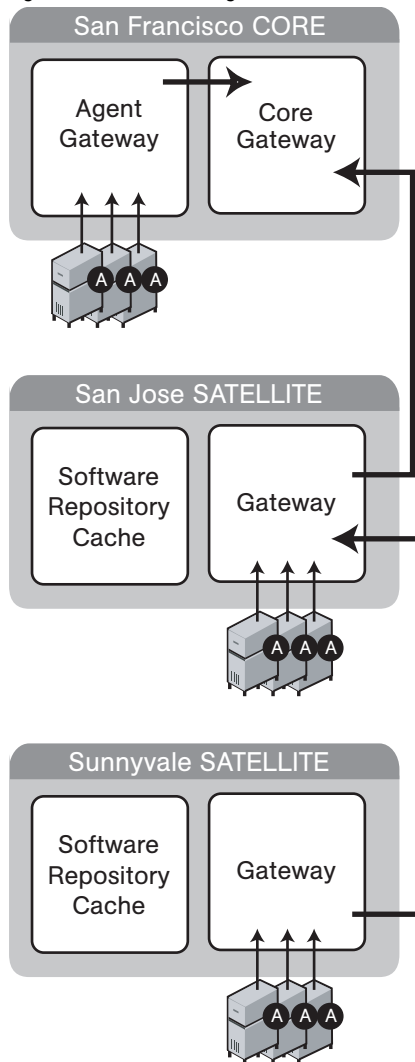


Figure 2-7 shows a Satellite connected to two cores in a multimaster mesh. A Satellite Gateway routes traffic to only one core Gateway at any given time. The Gateway chooses the route with the lowest cost, a parameter specified during Gateway installation. Suppose that the cost of the link between the 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 2-7: Satellite in a Multimaster Mesh

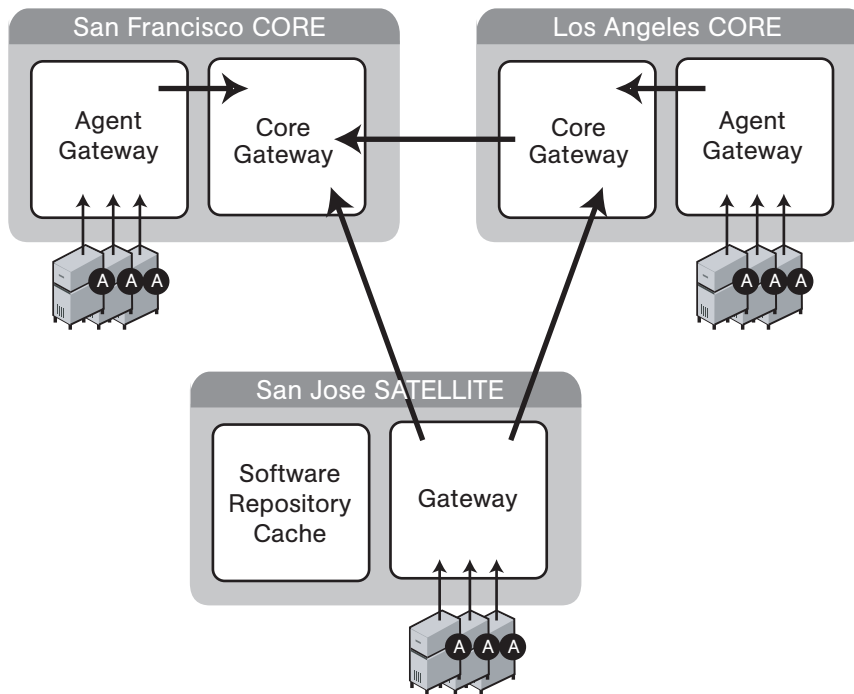
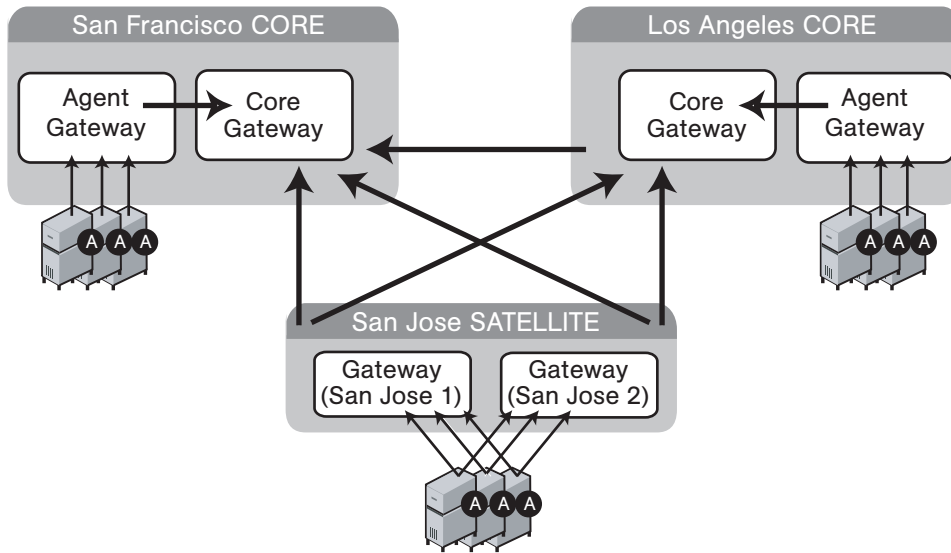


Figure 2-8 shows a topology that provides failover capability in two ways. First, the Gateway in each Satellite has connections to both core Gateways. If one core becomes unavailable, the other core can manage the servers in the Satellite. Second, the Agents in the Satellite point to both Satellite gateways. 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 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 2-8: Satellite With Multiple Gateways in a Multimaster Mesh



Chapter 3: Supported Operating Systems and Hardware Requirements

IN THIS CHAPTER

This chapter discusses the following topics:

- Supported Operating Systems
- Hardware Requirements for Opsware Core Servers

Supported Operating Systems

This section discusses the following topics:

- Supported Operating Systems for Opsware Core Servers
- Supported Operating Systems for Opsware Agents, Opsware Command Center, and 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 3-1: Opsware Core Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE CORE | VERSIONS |
|--|-------------------------------|
| Sun Solaris | Solaris 8 Solaris 9 |
| Red Hat Linux | Red Hat Enterprise Linux 3 AS |

The following table lists the supported operating systems for an Opware Satellite.

Table 3-2: Opware Satellite Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPWARE SATELLITE | VERSIONS |
|--|--|
| Sun Solaris | Solaris 9 |
| Red Hat Linux | Red Hat Enterprise Linux 2.1 AS Red Hat Enterprise Linux 3 AS |

Supported Operating Systems for Opware Agents, Opware Command Center, and 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.



For the supported operating systems for Opware Agents, Opware SAS supports Red Hat Linux 3 AS/ES/WS and Red Hat Linux 4 AS/ES/WS on both 32 bit (also known as i386) and 64 bit (also known as AMD64 or EM64) x86 architecture. All other versions of Red Hat Linux are supported on 32 bit architecture only.

Table 3-1: Opware Agent Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPWARE AGENT | VERSIONS |
|--|---|
| AIX | AIX 4.3 AIX 5.1 AIX 5.2 AIX 5.3 |
| HP-UX | HP-UX 10.20 HP-UX 11.00 HP-UX 11.11/11i |

Table 3-1: Opsware Agent Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT | VERSIONS |
|--|---|
| Sun Solaris | Solaris 6 Solaris 7 Solaris 8 Solaris 9 Solaris 10 |
| Fujitsu Solaris | Solaris 8 Solaris 9 Solaris 10 |
| Windows | Windows NT 4.0 Windows 2000 Server Family Windows Server 2003 |
| Red Hat Linux | Red Hat Linux 6.2 Red Hat Linux 7.1 Red Hat Linux 7.2 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 |
| SUSE Linux | SUSE Linux Enterprise Server 8 SUSE Linux Standard Server 8 SUSE Linux Enterprise Server 9 |

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

Table 3-2: OCC Client Supported Operating Systems

| SUPPORTED OPERATING SYSTEMS FOR OCC CLIENT | VERSIONS |
|---|--|
| Windows | Windows XP Windows 2000 Windows 2003 |

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 requirements for core servers follow:

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

See “Opware Core Scalability for Performance” on page 49 in this chapter for more information.

Memory Requirements

The memory requirements for core servers follow:

- 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 `/lc`.) 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 5.2 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 3-3 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 3-3: 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 | | | |
| 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

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 3-4 lists the approximate number of core servers required for a given number of managed servers and Opware users.

Table 3-4: Required Number of Core Servers

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

Scaling Opware SAS With a Multimaster Mesh

To support global scalability, you can install an Opware core in each major facility, linking the cores in a multimaster mesh. The size of the Opware 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 Opware Command Center. Therefore, the number and location of Opware Command Center instances is flexible. A common implementation is with two geographically distributed Opware 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 Opware 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 *Opware® SAS 5.2 Configuration Guide* for more information.

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.

Appendix A: Glossary

IN THIS APPENDIX

This appendix describes the terminology and the acronyms used within Opsware SAS.

ACM See Application Configuration Management.

Ad-Hoc scripts A script that is created (or uploaded) and then immediately executed by a user. The script is intended for one-time use and is not stored in Opsware SAS.

administrator See Opsware administrator.

Agent See Opsware Agent.

Agent Installer An application that installs the Opsware Agent on a server.

Agent Uninstaller An application that uninstalls the Opsware Agent on a server.

application configuration Contains application configuration templates associated with an application.

Application Configuration Management (ACM) An Opsware feature that enables you to manage and modify configuration files for applications on managed servers.

application Provisioning See Software Provisioning.

audit A process that compares Opsware managed servers to determine how objects may differ. When an audit reveals a difference between servers, you can install software and server objects to remediate the discrepancy.

audit job The process that performed the audit.

audit template A definition of source, one or more targets, and selection criteria that will be examined during the audit process to compare servers, server groups, and existing snapshots.

Automated Configuration Tracking An Opsware feature that allows users to monitor critical configuration files and configuration databases. When Opsware SAS detects a change in a tracked configuration file or configuration database, the system can perform a

number of actions, including backing up the configuration file or sending an email to a designated individual or group.

available patch A patch that the patch administrator has tested and marked as available. Only patches that have been marked as available can be installed by anyone other than a patch administrator. (The patch administrator can install an unavailable patch in order to test it.)

available server A reserve of new, unconfigured Opware-enabled servers ready for quick deployment. The provisioned server can be moved into the Live environment to replace existing servers, add capacity, or support new applications. While optional, provides faster recovery options in cases of hardware failure.

backup A feature in Automated Configuration Tracking that performs a backup of a file or database when it detects a change to a tracked configuration file or database. This action is performed only if the backup action is selected in the configuration tracking policy for the file or database.

backup (CDR) Process of saving the entire contents of the current Live directory for a specific service to the Backup directory. Code Deployment & Rollback (CDR) saves the backup copy to the local disk for the host on which the Backup operation was run. Only one backup copy is maintained at any time for a service.

backup event An event that causes configuration files or configuration databases to be backed up. Types of backup events include manual, full, and triggered.

blocked attachment An attachment that is not installed when that template is applied. The attachment also does not appear in child templates or folders.

Boot Server A part of the OS Provisioning feature that supports network booting of Sun and x86 systems with inetboot and PXE respectively. The processes used to provide this support include the Internet Software Consortium DHCP server, and Sun Solaris TFTP and NFS.

Build Manager A part of the OS Provisioning feature that facilitates communication between the OS Boot Agent and the Command Engine for OS provisioning.

CDR See Code Deployment & Rollback (CDR).

change log An audit trail of changes made to a node (read-only). Tracks changes made to a node. Identifies who has recently modified the node to add or remove software packages, add or remove operating systems, add or move servers, and create or remove subordinate nodes.

Code Deployment & Rollback (CDR) An Opware feature used to push updated code and content to staging host servers.

Code Deployment Role A specific role that authorizes access to capabilities and functions with the Opsware Code Deployment & Rollback feature.

Command Engine Topsware SAS component that enables distributed programs to run across many servers. The Command Engine handles the entry of scripts into the Opsware Model Repository (the script storage location in Opsware SAS) and the versioning of stored scripts. Command Engine scripts are written in Python and run on the Command Engine server.

Communication Test A feature that helps in identifying managed servers with unreachable Opsware Agents. A Communication Test lists all servers with unreachable agents, returns specific errors associated with each unreachable agent, and provides troubleshooting information to resolve the error. The Communication Test runs various tests like Command Engine to Agent Communication, Crypto Match, Agent to Command Engine Communication, Agent to Data Access Engine, Agent to Software Repository Communication, and Machine ID mismatch to determine if an Opsware Agent is reachable.

configuration template A set of values that represent the configuration file of an application.

configuration tracking policy The configuration tracking policy defines the set of files or configuration databases to be monitored, and the actions to be taken when change is detected to a tracked file.

configuration tracking reconcile Process by which new configuration tracking policies or changes to existing configuration tracking policies are deployed on servers.

core See Opsware core.

custom attributes Attributes such as miscellaneous parameters and named data values that users can set for servers in the Opsware Command Center. Used when performing a variety of Opsware functions, including network and server configuration, notifications, and CRON script configurations.

custom extension Custom Command Engine scripts that extend Opsware SAS functionality to customers to cover their specific needs.

customer An account within Opsware SAS that has access to designated resources, such as servers and software.

cutover A feature in CDR, that causes the Update directory and current Live directory to be identical. Performed automatically by determining the differences between the Update directory and current the Live directory. The files that are different are synchronized from the Update directory to the current Live directory.

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

data center Legacy term. See facility.

Data Center Intelligence Reporting An interface for mining the data that is contained in the Model Repository about all managed servers.

deactivated server Server removed from Opsware management even though its history still exists.

deployment Within CDR, automatically pushes code and content from a staging server to a live network server.

deprecated A possible state of a package or patch in Opsware SAS. A deprecated package or patch can no longer be installed on a managed server, but might still be installed on a server before the patch or package was deprecated.

device Legacy term. See server.

Distributed Scripts An Opsware feature that allows you to manage scripts in your managed environment.

Dormant Opsware Agent An Opsware Agent that runs in the dormant mode after its installation when Opsware SAS core is not available on the network. The dormant agent periodically attempts to contact the core and when the core is available, it performs the initialization tasks to complete its installation.

dynamic group A server group that contains servers added to or removed from the group based on a set of user-defined rules.

email notification list In the Automated Configuration Tracking feature, an email can be sent to the email addresses in the email notification list whenever a change to a tracked file or configuration database is detected.

Environment Tree The Environment Tree manages characteristics about a customer's unique data center environment, including hardware, location of servers, network infrastructure, application names, business units, and service levels assigned to servers and applications. The information contained in the Environment Tree, combined with the information contained in the Software Tree, is utilized by the Opsware Automation Platform to model and simulate operational changes before they are executed in the production environment.

facility The collection of servers that a single Opsware core manages. A facility can be all or part of a data center, server room, or computer lab.

full backup During a full backup, all tracked configuration files that were selected to be backed up are backed up (and not just the files that have changed). Full backup is performed if you select backup as the action for a tracked configuration file.

full reconcile A reconcile process that reconciles a server with all of the nodes that it has been assigned to.

gateway See Opsware Gateway.

Global Shell A terminal window for the Opsware Global File System (OGFS) in your Opsware SAS.

group See server group.

IDK Intelligent Software Module (ISM) Development Kit. The tools from Opsware Inc. used to build and upload ISMs.

Import Media tool A utility script included with Opsware SAS that is used to import OS media from the Media Server to Opsware SAS.

inclusions/exclusions criteria Specifies how to include and exclude directories and files during the snapshot or audit process.

incremental backup During an incremental backup, only targets that have changed since the last backup (and that have been selected to be backed up) are backed up. Incremental backup is performed if you select backup as the action for a tracked configuration file.

inherited attachment An attachment that is inherited from an ancestor folder or a template.

initialization Legacy term. See OS Provisioning.

IP Range Groups A designated set of servers assigned to a customer account, grouped by either a physical or a logical list.

IP Ranges A designated grouping of servers.

ISM Intelligent Software Module. A set of file and directories that include application bits, installation scripts, and control scripts. When an ISM is uploaded into an Opsware core, a node is created for the application and installable packages are attached to the node.

ISM control A script within an ISM package that can be run on a managed server.

job Any major process run by the Opsware Command Center or the Opsware Command Center Client such as Communication Test, Install Software.

Live directory In CDR, the directory that stores the actual code and content required to run a live site.

local attachment An attachment that is attached directly to a folder or a template.

MAC See Media Access Control Address (MAC).

Machine ID (MID) A unique identifier that Opware SAS uses to identify the server. Opware SAS assigns a unique number to the server when it first registers and stores the Machine ID and uses it to identify each server.

managed server A Server that has an Opware Agent installed on it and is under the control of a particular Opware core.

management IP The IP address that Opware SAS uses to communicate with the Opware Agent on the server.

manifest Within CDR, a list of files that indicate the results or preview of an update to be performed. Each entry in the list specifies the file size, last-modified date and timestamp, and the full directory path to the listed file.

Media Access Control Address (MAC) The network interface card's unique hardware number. The MAC is used as the server's physical address on the network.

Media Resource Locator (MRL) A network path in URL format that is registered with Opware SAS. The path defines the installation media for an OS.

Media Server Contains the vendor-supplied OS media used during OS provisioning over the network. The OS media on the Media Server is accessed over the network by using NFS for Linux and Solaris OS provisioning, and by using SMB for Windows OS provisioning.

MID See Machine ID.

Model Repository The Opware database that stores information about managed server configurations within Opware SAS. It contains all information necessary to build, operate, and maintain an Opware-managed site, including a list of all servers under management, the hardware associated with these servers, including memory, CPUs, storage capacity, and the configuration of these servers, including IP addresses, DNS configuration, and so on.

Model Repository Multimaster Component The application that propagates and synchronizes changes from each Model Repository database to all other Model Repository databases.

Modeling and Change Simulation Engine Opware SAS enables users to first model and simulate proposed operational changes to their environment before propagating

these changes to production servers and applications. Utilizing the information contained in the Software and Environment Trees, the Modeling and Change Simulation Engine maintains a model of the various hardware and software configurations and other customer characteristics associated with each of the production servers under Opsware SAS's control.

MRL See Media Resource Locator (MRL).

multimaster core An Opsware core that belongs to a multimaster mesh.

multimaster infrastructure component See Model Repository Multimaster Component.

multimaster mesh A set of two or more Opsware cores that are linked by synchronizing the data in the Model Repositories at each of the cores. The Model Repositories in each of the cores are continually updated so that they are exact duplicates of each other. All the Opsware cores in a multimaster mesh can be managed through a single Opsware Command Center.

My Jobs A page in the Opsware Command Center that displays a list of jobs from the Model Repository such as software installation or server provisioning.

My Scripts Private scripts that can only be executed by the user who created the script. My Scripts are created for personal use.

name-value pairs Legacy term. See custom attributes.

node A hierarchical set of categories or types that classify hardware, software, configuration, or other components of a site's infrastructure. Simplifies server management (for example, servers within Opsware SAS) and the software applications and configurations associated with those servers.

node-based configuration tracking policy A configuration tracking policy defined for a particular software node for a particular application.

OCLI See Opsware command Line Interface (OCLI).

OGFS See Opsware Global File System.

Opsware administrator Responsible for overall administration, policy, and practices for individuals accessing Opsware SAS. Can add users and define access to specific Opsware SAS features that allow users to view site information and deploy new code and content to their site.

Opsware Agent Intelligent software on Opsware-managed servers that is used to make changes to the servers. Depending on the request, might use global Opsware services. Some functions supported include software installation and removal, software and hardware configuration, server status reporting, and auditing.

Opware Automation features Opware SAS is made up of a set of Opware Automation features. Opware Automation features are the components that automate particular IT processes. The Opware Automation features include the following functions: Software Provisioning, Patch Automation, Configuration Tracking, Code Deployment and Rollback, Script Execution, and Data Center Intelligence Reporting.

Opware Discovery and Agent Deployment A feature that helps deploy Opware Agents to a large number of servers through the Opware Command Center Client.

Opware Command Center Web-based user interface for managing the Opware environment.

Opware Command Line Interface (OCLI) An alternative interface to the Opware Command Center. The OCLI allows you to perform some actions not possible through the browser-based interface of the Opware Command Center, such as uploading multiple packages, patches, AIX filesets, and so forth, in a batch operation.

Opware core The server side of Opware SAS server-agent architecture. A core consists of the Opware components (such as the Model Repository, the Software Repository, the Data Access Engine, and the Command Engine) for a particular installation.

Opware Gateway Provides connectivity with an Opware core either directly or through a network of gateways. All traffic between the servers in the Satellite and the core that manages them is routed through Opware Gateways.

Opware Global File System (OGFS) The Opware Global File System is a single, unified file system view of all file systems for all managed servers in Opware SAS.

Opware installation Either a standalone core, multimaster core, or Opware Satellite.

Opware model space The Opware Global File System (OGFS) file system structure that is derived from the Model Repository.

Opware 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.

Opware SAS The server management application to preserve the knowledge of system administrators, network engineers, and database administrators in a centralized knowledgebase. Automates previously manual tasks associated with the deployment, support, and growth of a data center infrastructure.

OS Build Agent A part of the OS Provisioning feature that is responsible for registering bare metal servers in Opware SAS and guiding the installation process.

OS media Installation software for an OS from the software vendor that is distributed on a CD-ROM, or DVD, or can be obtained by downloading the software from the vendor's FTP site.

OS Provisioning Process of installing a basic set of software components, including an operating system and an Opware Agent to add a server into the Opware managed environment. After provisioning is complete, the server is ready to be managed by Opware SAS.

Package Repository Legacy term. See Software Repository.

package A collection of executables, configuration, or script files that are associated with an Opware-installable application or program. In Opware SAS a package contains software package files registered in the Software Repository. Contains software for operating systems, applications (for example, BEA WebLogic, IBM WebSphere), databases, customer code, and software configuration information.

packaging server A managed server that has the IDK installed on it. Visual Packager requires a packaging server for each type of operating system for the packages you plan to create.

partial reconcile A reconcile process that only reconciles servers based on the nodes that the user has currently selected.

patch management administrator Administrator responsible for testing patches and defining patch options, such as installation and uninstallation scripts. A patch cannot be installed by other personnel until the patch administrator has marked the patch available through the Opware Command Center.

Patch Management An Opware feature that allows you to upload, test, and deploy patches in a safer and uniform way.

permission A setting within a User Group that allows or disallows access to Opware SAS features and resources. A resource is usually a set of managed servers or software nodes. The set of managed servers corresponds to a facility, customer, or server group.

platform The name and version of an operating system.

post-install script A shell script invoked on a managed server immediately after a software package is installed on a managed server.

post-uninstall script A shell script invoked on a managed server immediately after a software package is removed from the managed server.

pre-install script A shell script invoked on a managed server immediately before a software package is installed on a managed server.

pre-uninstall script A shell script invoked on a managed server immediately before a software package is removed from the managed server.

preview reconcile Before Opsware SAS installs software on a server, it performs a preview reconcile, and determines what will happen when the actual reconcile is performed (for example, what packages will be installed or removed, what server reboots are required, and so forth.)

primary IP A locally-configured IP address of the management interface.

private group A type of server group that can be edited, or deleted by the Opsware user who created the server group.

privileges See Permissions and User Group.

public group A type of server group that can be created, edited, or deleted by any Opsware user who has Manage Public Server Groups permissions.

realm One or more Opsware Gateways service the managed servers contained within an Opsware realm. In Opsware SAS, a realm is a routable IP address space, which is serviced by one or more gateways. All managed servers that connect to an Opsware core via a gateway are identified as being in that gateway's realm.

reconcile Process of updating the actual software configuration of a server based on the specified configuration stored in the Model Repository.

reconcile output After a reconcile operation completes, Opsware SAS displays the reconcile output for each server that was reconciled. The reconcile output aggregates output from the various installation, uninstallation, or post-installation scripts, messages from Opsware SAS, and messages from the system utilities that reconcile uses to perform the installation and uninstallation of packages, operating systems, and patches.

Reconcile Software Wizard A Wizard that can enable a user to directly invoke the reconcile process on a selected server or a group of servers.

reference server A managed server that is compliant (performs as expected) and is also referred to as a known working server or a baseline server.

remote terminal A terminal window for a Unix server or an RDP client window for a Windows server.

restore A function of the Automated Configuration feature that allows the user to return the configuration file or database to a previous state, when the backup action for a tracked file or database is selected.

restore Within CDR, the process of restoring the previous Live directory from the Backup directory to the Live directory.

restore queue Queue in which configuration files are placed before they are restored to a server.

Role Legacy term. See node or user group.

rollback Within CDR, returns a site to the state prior to the last cutover. During rollback, restores the set of modified and deleted files to the Live directory.

rosh The remote Opsware shell is a command that makes a client connection enabling you to remotely run programs on managed servers.

Satellite See Opsware Satellite

Script Execution See Distributed Scripts.

selection criteria Rules that instruct Opsware SAS what server objects you want to collect information about, how to collect the server objects, and (optionally) file comparison and inclusions/exclusions criteria. Selection criteria is required for the snapshot and audit processes.

sequence Process within CDR that simplifies deployment by grouping a collection of service operations and synchronizations that can be performed as a single task.

Sequence Editor In CDR, a predefined User Group to create, modify, or delete a sequence definition.

Sequence Performer (Production) In CDR, a predefined User Group to directly perform or request performance of a sequence action on production hosts.

Sequence Performer (Staging) In CDR, a predefined User Group to directly perform or request performance of a sequence action on staging hosts.

Sequence Requester (Production) In CDR, a predefined User Group to request performance of a sequence action on production hosts.

Sequence Requester (Staging) In CDR, a predefined User Group to request performance of a sequence action on staging hosts.

servers Any specific hardware. Specific nodes are attached to servers that determine the specific software, configuration, and other server attributes.

server assimilation Opsware SAS assimilates servers that are already functioning in the operational environment, which allows users to deploy and manage new applications installed on those servers. Assimilating servers installs Opsware Agents on the servers and registers them with the Model Repository.

server baselines Process of defining and provisioning servers with standard configurations. Opware templates can be used to automate the building of complete server baselines.

Server Explorer A feature of the Opware Command Center Client that allows you to browse and manage servers and server groups in your facility.

server group A feature used to organize servers into groups in order to perform the same action on all of the servers. Server groups can be comprised of individual servers as well as other server groups.

Server ID The primary key in the Opware Model Repository that represents a given server. The Server ID is used internally in Opware SAS.

server lifecycle The various server states assigned to a server by Opware SAS. Server states include Unprovisioned, Available, Installing OS, and Managed.

server management Process by which users can manage and track servers in an Opware-managed environment. Opware SAS forces changes to the operating environment by first changing the centralized configuration information in the Model Repository and then changing the actual configuration of physical servers.

Server Pool Servers that have registered their presence with Opware SAS but do not have a full operating system installed.

server provisioning Process of installing a basic set of software components that include the operating system, an Opware Agent, and other system utilities and debugging tools to manage the server. Configuration is defined in the Model Repository.

server reconcile A process that compares a designated server image from the Model Repository with a specific server, checking for configuration, content, versions, and so forth, to determine if the live server is current and up-to-date. Includes OS, applications, upgrades, and patches.

Server Search A Feature that allows you to search for servers based on a variety of criteria, including OS version, installed package, customer, and installed patch.

Server Status Feature that defines server availability. The three major status conditions are USE, STAGE, and STATE.

server-based configuration tracking policy A configuration tracking policy that is defined for a particular server or group of servers, rather than for a particular software node (application).

service A host application (for example, BEA WebLogic, Allaire ColdFusion, Microsoft IIS, Apache Web Server, or iPlanet Application Server).

Service Editor In CDR, a predefined User Group to define and modify or delete service definitions.

Service Performer (Production) In CDR, a predefined User Group to directly perform or request performance of service operations on production hosts (servers).

Service Performer (Staging) In CDR, a predefined User Group to directly perform or request performance of service operations on staging hosts.

Service Requester (Production) In CDR, a predefined User Group to request performance of service operations on production hosts.

Service Requester (Staging) In CDR, a predefined User Group to request performance of service operations on staging hosts.

service-instance Multiple independent instances of a service running on a host (for example, BEA WebLogic, which can run single or multiple instances).

Service Levels User-defined categories that are used to group servers in an arbitrary way. For example, a user can group servers by functionality, tier, application, or ontology.

Shared Scripts Public scripts that every Opsware SAS user can access.

Site Backup directory In CDR, the directory that stores a complete backup of the Live directory when the user issues a Backup service operation.

Site Previous directory In CDR, the directory that stores the files that have changed between the current Live directory and its previous state prior to the last cutover. It holds all the changes necessary to revert the Live directory back to the state that it was in before the last cutover.

snapshot A record of how an Opsware managed server is configured at a particular point in time. Snapshots allow administrators to audit the configuration of servers and deploy files and software to correct discrepancies. A snapshot can be based on specified server objects. Server Compliance records one snapshot per server.

snapshot job The process that created a snapshot of a server or server group.

snapshot template A definition of a target and selection criteria that will be examined during the snapshot process to capture and record information about a managed server.

Software Provisioning An Opsware feature that allows system administrators to install, configure, and remove packaged software in a systematic way across servers that are distributed over many different facilities. Software provisioning can also involve the automatic execution of installation and post-installation scripts. Softwares can be provisioned by using the Install Software Wizard, the Install Template Wizard, or by attaching a server to a node and then reconciling the server.

Software Repository The central repository for all software managed by Opware SAS. It contains software packages for operating systems, applications, databases, customer code, and software configuration information.

Software Repository Cache An Opware Satellite component that contains local copies of files. The Software Repository Cache stores files from the Software Repository of an Opware core or from another Software Repository Cache, and supplies the cached files to Opware Agents on managed servers.

Software Repository Replicator A component providing backup functionality for Software Repositories running in a multimaster mesh.

Software Tree The Software Tree records a variety of information for software applications and operating systems, including data about how changes to a given software application might impact other existing applications.

source In the snapshot process, this is the managed server that information is recorded about. In the audit process, this is an existing snapshot or server you are comparing selection criteria *from*.

standalone core An Opware core that manages servers in a single facility. Unlike a multimaster core, a standalone core does not communicate with other cores.

static group A server group in which the servers are added to and removed from the group manually.

synchronization Process within CDR to move modified files from a directory on a source host to a directory on a destination host.

Synchronization Editor In CDR, a predefined User Group to create, modify, or delete a synchronization definition.

Synchronization Performer In CDR, a predefined User Group to directly perform or request performance of a synchronization action.

Synchronization Requester In (CDR), a predefined User Group to request performance of a synchronization action.

target In the snapshot process, this is the managed server or server group you are recording information *about*. In the audit process, this is an existing snapshot, server, or server group you are comparing selection criteria *to*.

template Used to install a set of (usually related) applications through a single invocation of a wizard.

template inheritance Process by which templates and folders inherit all attachments of the folder they reside in. Inheritance is propagated from parent (folder) to child (template or folder) and to all children of children.

tunnel A TCP connection between two Gateways that carries multiplexed TCP or UDP connections.

Update directory The directory that CDR writes to when synchronizing modified files in source and destination hosts. After synchronization, the Update directory is different from the current Live directories. After cutover, the Update directory and current Live directory are identical.

user An individual with access to Opsware SAS. An Opsware user belongs to one or more User Groups, which control the access of its members..

User Group Represents a role played an organization's Opsware users. The permissions specified for a user group determine what the group's members can do with Opsware SAS.

Value Set Editor Enables you to change the values in a configuration file by editing that file's value set. Each entry configuration file is represented inside the value set editor as a "value set" (a key name and a value).

Web Service API A Web services interface to facilitate the integration of operations and business support systems with Opsware SAS. The Opsware Web Services APIs allow other IT systems, such as customers' existing monitoring, trouble ticketing, billing, and virtualization technology, to exchange information with Opsware SAS.

Web Services Data Access Engine A Web services interface to the Model Repository that provides increased performance to other Opsware SAS components.

Wizard Graphical user interface that groups a series of data collection operations, actions, and jobs into a logical, easy-to-understand workflow presentation.