OPSWARE INC
Automating IT™

Opsware® SAS 5.2 Configuration Guide

Corporate Headquarters

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

Table Of Contents

Preface xxi

Chapter 1: Opsware SAS Overview 1

Chapter 7: Package Management 187

Chapter 12: Code Deployment Setup 349

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

This guide describes how to set up Opsware SAS features after an Opsware core has been installed in a facility. Specifically, this guide describes how to set up users, user groups, administrators, customers, and facilities. it discusses how to set up Opsware SAS features, such as OS Provisioning, Patch Management, Software Provisioning, Code Deployment and Rollback, and Configuration Tracking, and how to manage packages in the Software Repository.

Contents of This Guide

This guide contains the following chapters and appendices:

Chapter 1: Opsware SAS Overview: provides a high-level overview of the entire Opsware SAS, including each Opsware SAS features and a description of the types of users who interact with Opsware SAS.

Chapter 2: Opsware SAS Configuration: provides information about the supported browsers for the Opsware Command Center and how to set several configuration parameter values that Opsware SAS uses to send email notifications and alerts, and to display the Opsware administrator contact information.

Chapter 3: User and Group Setup: provides information about how to create and delete users, user groups, and administrators and how to assign permissions to each.

Chapter 4: Server Management Configuration: provides information about how you can control server management in your operational environment by creating customers to associate servers with, creating and modifying server attributes to categorize the servers running in your operational environment, and by creating IP address groups to control which customers your servers are associated with when you install the Opsware Agent on them.

Chapter 5: OS Provisioning Setup: provides a description of all tasks necessary to prepare for operating system provisioning including media management, operating system specific tasks, operating system definitions, build customization scripts, OS build process default definitions, operating system definitions in templates, and details of hardware support.

Chapter 6: OS Installation Integration: provides a description of how Opsware SAS handles OS installation integration with third-party installation technologies, how to perform integration including Opsware Agent Installer commands and options, and how to integrate with specific operating system installation technologies.

Chapter 7: Package Management: provides information about container and installable packages, and details about package types, metadata, and any prerequisites or scripts for each supported operating system. It also discusses how to view packages assigned to nodes, and how to upload, overwrite, edit, delete, deprecate, and download packages.

Chapter 8: OCLI Version 1 for Package Management: provides information about installing the Opsware CLI, file transfer commands, command syntax, command options, and supported operating systems and package types.

Chapter 9: Software Repository Replicator Setup: describes how to set up the Software Repository Replicator to enable backup functionality for Software Repositories running in a multimaster mesh.

Chapter 10: Software Provisioning Setup: provides information about how to prepare for provisioning servers with software including a description of the Software Tree, managing nodes on the Software Tree, an overview of modeling software attached to nodes, configuration settings, viewing software attached to nodes, adding and removing software packages from nodes, and changing the installation order of software. It also discusses the concepts of inheritance and dependencies. Managing custom attributes is described, as well as an in-depth discussion of all aspects of creating templates for operating systems, patches, applications, and service levels.

Chapter 11: Patch Management Configuration: provides information about managing patches including testing and installation standardization, operating systems and patch types, the roles of the patch administrator and system administrator in applying patches, and the permissions required for performing patch management. It also describes how to set up the patch management system, upload patches, and the administration of patches by using the Opsware Command Center.

Chapter 12: Code Deployment Setup: provides information about setting up services, synchronizations, and sequences in the Code Deployment and Rollback (CDR) feature to deploy code and content to managed servers.

Chapter 13: Automated Configuration Tracking Setup: provides information about configuration tracking policies, the supported types of configuration files and databases that can be backed up, how changes are detected, node-based tracking policies, and reconciling node-based tracking policies.

Appendix A: Permissions Reference: provides information about which Opsware SAS permissions to grant Opsware users so that they access only the areas of functionality relevant to their responsibilities in the managed server environment. If access is allowed to a functional area in the Opsware Command Center, the link for that function displays in the navigation panel and on the home page.

About Opsware Documentation

Conventions in This Guide

This guide uses the following typographical and formatting conventions.

NOTATION	DESCRIPTION
`Courier`	Identifies text of displayed messages and other output from Opsware programs or tools.
`Courier Bold`	Identifies user-entered text (commands or information).
`Courier Italics`	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 *Opsware® 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 *Opsware® SAS 5.2 Administration Guid*e is intended to be read by Opsware administrators who will be responsible for setting up accounts for users, creating user groups and additional Opsware administrators, assigning permissions for different

levels of operation and access, adding customers and facilities, and monitoring and diagnosing the health of the Opsware SAS components.

- The *Opsware® SAS 5.2 Deployment and Installation Guide* is intended to be used by system administrators who are responsible for the installation of Opsware SAS in a facility. It documents how to run the Opsware Installer and how to configure each of the components.
- The *Planning Deployments for Opsware® SAS 5.2* is intended to be used by advanced system administrators who will be responsible for planning all facets of an Opsware SAS installation and deployment. It documents all the main features of Opsware SAS and scopes out the planning tasks necessary to successfully deploy Opsware SAS. Sections include: planning the Opsware 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 *Opsware® SAS 5.2 Configuration Guide* is intended to be used by system administrators who are responsible for all facets of configuring the Opsware Command Center. It documents how to set up users and groups, configure Opsware server management, and setting up the main Opsware Command Center features, such as patch management, configuration tracking, software repository replicator setup, code deployment, as well as OS and software provisioning.

Contacting Opsware, Inc.

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

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

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

- https://download.opsware.com/opsw/main.htm

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

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

The Opsware Customer Support email address and phone number follow:

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

Chapter 1: Opsware SAS Overview

IN THIS CHAPTER

This chapter discusses the following topics:

- Opsware SAS Overview
- Opsware SAS Features

Opsware SAS Overview

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.

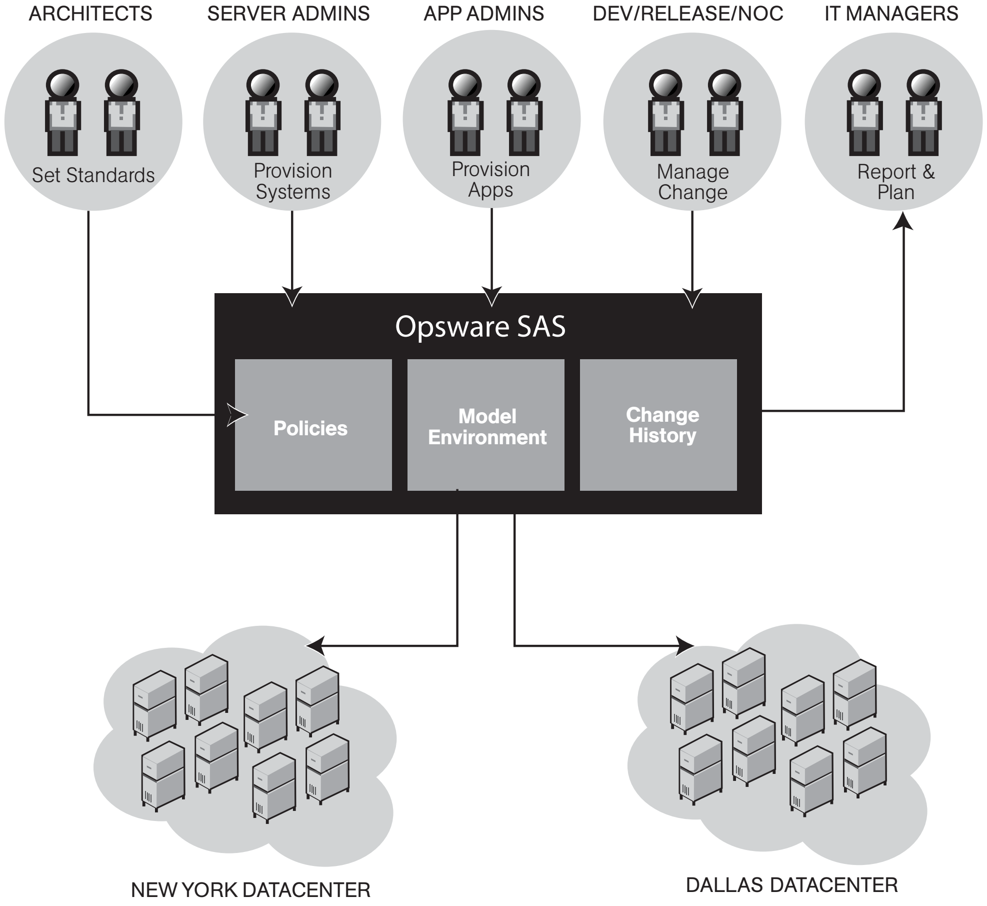
Opsware SAS does not just automate your operations, it also allows you to make changes more safely and consistently, because you can model and validate changes before you actually commit the changes to a server. Opsware SAS also helps ensure that modifications to your servers work on your first time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

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

Table 1-1: Types of Opsware 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 Opsware 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 Opsware 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 Opsware SAS documentation, these users are referred to as Opsware users or system administrators. These users log into the Opsware Command Center and OCC Client and use these user interfaces to manage servers in their IT environment.
- **Opsware Administrators** are the users, with special training and information, who are responsible for installing and maintaining Opsware SAS. In the Opsware SAS documentation, these users are referred to as Opsware administrators. They use the Administration features in the Opsware Command Center to manage Opsware SAS and Opsware users (by adding user accounts and assigning permissions for different levels of operation and access), to add customers and facilities, and to change Opsware SAS configurations. They monitor and diagnose the health of Opsware SAS components. Opsware administrators need to understand how Opsware SAS features operate to support users and Opsware SAS.
- **Policy Setters** are the power users who are responsible for architecting what Opsware 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.

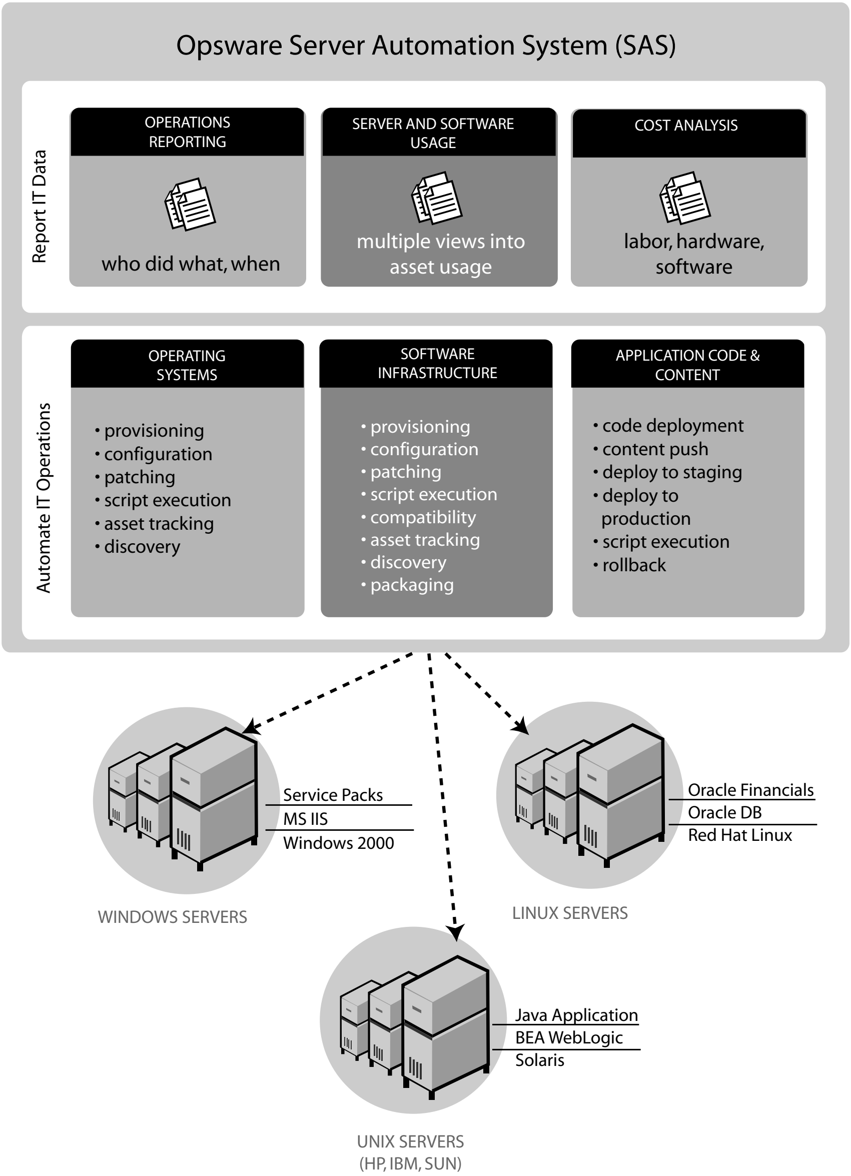
The features are designed to replace ad hoc, error-prone, manual processes. For example, by using the OS Provisioning feature, users can set standards for different types of servers and automatically provision the servers, saving time and ensuring that operating system builds are consistent. By using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

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
- Server Compliance
- Application Configuration Management

All Opsware 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: Opsware 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. Opsware 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 Opsware 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, Opsware 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, Opsware 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 trial, and the ability to roll back changes, all contribute to Opsware 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 Opsware 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**

  Opsware 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 Opsware 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**

  Opsware 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**

  Opsware 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**

  Opsware SAS maintains a comprehensive audit trail of the software that Opsware users install, configure, and remove from a server. When combined with the additional events that Opsware 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**

  Opsware 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 Opsware 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.

Opsware SAS has a deep understanding of native patch formats and structure. System administrators upload patches directly into Opsware 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

Opsware SAS automates code and content deployment to reduce the risk and time requirements associated with pushing new code to production. The Code Deployment & Rollback (CDR) feature provides an automated system for deploying code (such as, ASP, JSP, JAR, Java, C++, and Perl files) and content (such as, HTML, JPEG, GIF, and PDF files). Specifically, CDR 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 Opsware SAS notices a server configuration change, it can log the change, notify administrators about the change with email, or back up the configuration, depending on the policy set by the administrator.

When a bad configuration change forces administrators to roll back to a previous version, they can use Opsware SAS to restore the configuration file to the saved version of the configuration. By notifying users about configuration changes – and maintaining a version history of those changes – organizations can quickly diagnose problems related to configuration errors and 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 Opsware-managed servers. By executing scripts with Opsware SAS instead of manually, administrators benefit by using the following features:

- Parallel script execution across many Unix and/or Windows servers, saving time and ensuring consistency
- Role-based access control, ensuring only authorized administrators can execute scripts on hosts to which they have access
- The ability to control access to scripts by storing them in private or in public libraries
- The ability to see and download script output one server at a time or in a consolidated report, which captures output from all servers in a single place
- The ability for scripts to be mass-customized 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 though 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.

Opsware 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 Opsware SAS. Opsware 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 *Opsware*® 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 Opsware Data Center Intelligence Reporting component is an optional component. By default, it is not installed with Opsware SAS. If this reporting component is not available for your organization, contact your Opsware 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 Opsware Discovery and Agent Deployment (ODAD) feature allows you to deploy Opsware agents to a large number of servers in your facility and place them under Opsware management.

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

- Scan your network for servers on the network.
- Select servers for Opsware 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 Opsware 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

Opsware 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 Opsware data model to set configuration values.
- Manage configurations of any application by building configuration templates.

Global Shell

The Opsware Global Shell feature is intended for the Opsware 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 Opsware SAS. The file system is known as the Opsware 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.

Chapter 2: Opsware SAS Configuration

IN THIS CHAPTER

The topics covered in this chapter include:

- Supported Browsers for the Opsware Command Center
- System Configuration
- Ways to Use Opsware SAS Configuration Parameters

Supported Browsers for the Opsware Command Center

The following table lists the supported browsers for the Opware Command Center.

Table 2-1: Supported Browsers for the Opsware Command Center

BROWSER	WINDOWS 2000	WINDOWS 2003	WINDOWS XP	LINUX 6.2+	SOLARIS 6 +	MAC OS X
Microsoft Internet Explorer 5.5	X					
Microsoft Internet Explorer 6.0	X	X	X			
Mozilla 1.6	X	X	X			
Firefox 1.0	X	X	X			

Configuring Your Browser

In order to run the Opsware Command Center, your browser must be configured as follows:

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

System Configuration

During the installation of an Opsware core the Opsware Installer sets specific system configuration parameters. In addition to the parameters that are set during installation, there are also many default values for the various system configuration parameters that should not be changed unless expressly directed to do so by Opsware Inc.

For information about how to use this function when you install an Opsware core, see the *Opsware® SAS 5.2 Deployment and Installation Guide.*

The Opsware Agent reads the system configuration values at installation time only. If any of the configuration values change, the agent configuration must be updated manually. Contact Opsware, Inc. Technical Support for help making these changes, or in making any other changes in the System Configuration area of Opsware SAS.

Ways to Use Opsware SAS Configuration Parameters

This chapter documents how to set specific parameters after you install an Opsware core so that Opsware SAS properly sends email alerts and displays the correct support contact information for your organization.

Where a value for a configuration parameter *must* be set for an installation of an Opsware core, *Opsware® SAS 5.2 Deployment and Installation Guide* provides instructions for setting the value. Set configuration values for those parameters as *explicitly* directed by the steps in the installation procedures.

⚠ Do not change other configuration values, unless *explicitly* directed to do so by this guide or by *Opsware® SAS 5.2 Deployment and Installation Guide* or by your Opsware, Inc. Support Representative.

After you install an Opsware core, you should set several configuration parameter values that Opsware SAS uses to send email notifications and alerts, and to display the Opsware administrator contact information.

These values are set by selecting Administration ➤ System Configuration in the Opsware Command Center.

Configuring Contact Information in the Opsware Help

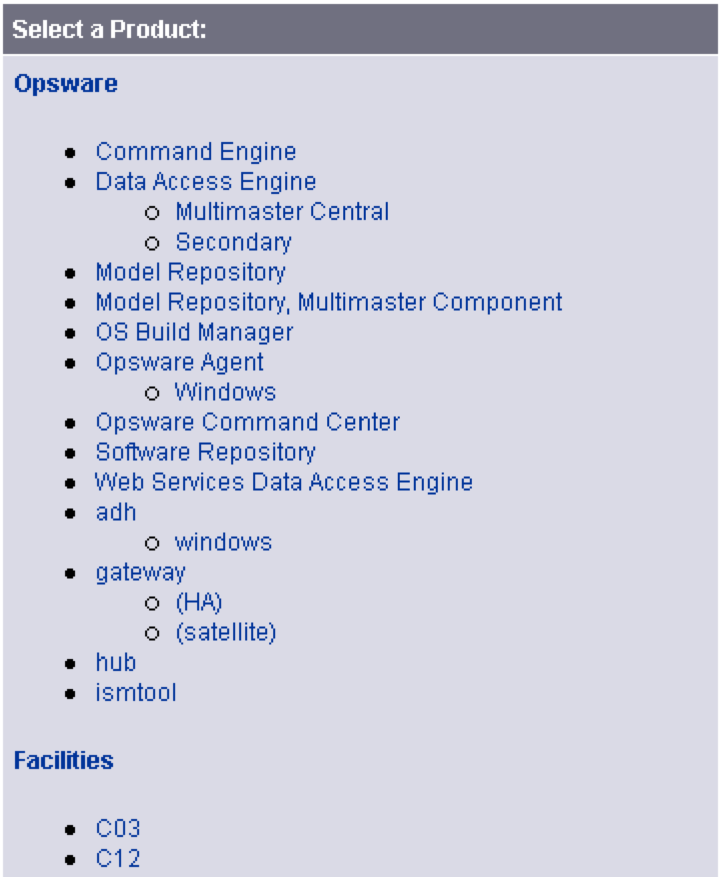
Perform the following steps to configure the Opsware administrator contact information that appears in Opsware SAS Help page:

1. Login to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears, as Figure 2-1 shows.

Figure 2-1: Select a Product page in Opsware SAS Configuration



Select a Product:

Opsware

- Command Engine
- Data Access Engine
  - Multimaster Central
  - Secondary
- Model Repository
- Model Repository, Multimaster Component
- OS Build Manager
- Opsware Agent
  - Windows
- Opsware Command Center
- Software Repository
- Web Services Data Access Engine
- adh
  - windows
- gateway
  - (HA)
  - (satellite)
- hub
- ismtool

Facilities

- C03
- C12

3. Under Select a Product, click the link for the Opsware Command Center. The configuration page for the Opsware Command Center appears.

4. Configure the following contact information by setting these parameters:

   - In the field **owm.name.opswareadministratorphonenumber**, enter the telephone number for your organization's Opsware SAS support.

   - In the field **owm.name.opswareadministratoremail**, enter the email address for your organization's Opsware SAS support.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

Configuring the Mail Server for a Facility

Perform the following steps in an Opsware multimaster mesh to configure the mail server for the core running in *each* facility.

1. Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click the link for the facility name. The configuration page for the facility appears.

   Opsware components use the parameter `opsware.mailserver` to determine the address of the mail server to use. If a value is not entered in the field, by default, the value of `opsware.mailserver` is smtp. If managed servers are able to contact a mail server by using this name as the address, then you do not need to modify this parameter.

4. In the field **opsware.mailserver**, enter the host name of the mail server.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

6. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

7. Under Select a Product, click Command Engine.

8. In the field **way.notification.email.fromAddr**, enter the “From” email address for the email messages that will be sent by the Command Engine to notify users about scheduled jobs.

9. Click Save to apply the changes.

10. Restart the Command Engine and Opsware Command Center.

11. If Opsware SAS is running in multimaster mode, restart the Model Repository Multimaster Component.

When restarting multiple Opsware components, you must restart them in the correct order. See the *Opsware® SAS 5.2 Administration Guide* for information about the correct restart sequence for Opsware SAS components.

Setting Email Alert Addresses for an Opsware Core

✓ You should configure these email alert addresses before you install an Opsware Agent on the servers in your operational environment because the Opsware Agent on a managed server will *only* read this email configuration information the first time it contacts Opsware SAS.

Perform the following steps to configure these email alert addresses. The Opsware Installer installs an Opsware core with placeholder values (EMAIL_ADDR) for these parameters.

1. Login to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click the Opsware Agent link. The configuration page for the Opsware Agent appears.

4. Configure the following required email alert addresses:

   - In the field **acsbar.ErrorEmailAddr**, enter the address that Opsware SAS will send warning emails to when any configuration tracking limit is exceeded (for example, when the configuration tracking feature stopped backing up configuration files and databases).

   - In the field **acsbar.emailFromAddr**, enter the address that the Opsware Agent will use as the email From address in the emails when Opsware SAS detects a tracked configuration change.
     Recommendation – use agent@yourdomain.com.

- In the field **CronbotAlertAddress**, enter the email address that the Opsware Agent will use to alert the recipient about failed scheduled jobs.
- In the field **CronbotAlertFrom**, enter the email address that the Opsware Agent will use as the email From address in the emails about failed scheduled jobs. Recommendation – use agent@yourdomain.com.

5 Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

Configuring Email Alert Addresses for Multimaster

Perform the following steps to configure email alert addresses for multimaster. The Opsware Installer installs an Opsware core with placeholder values (EMAIL_ADDR) for these parameters.

1 Log in to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2 From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3 Under Select a Product, click the Model Repository, Multimaster Component link. The configuration page for the Model Repository, Multimaster Component appears.

4 Configure the following email parameters:

- In the field **sendMMErrorsTo**, enter the email address to which multimaster conflicts will be sent.
- In the field **sendMMErrorsFrom**, enter the address that Opsware SAS will use as the email From address in the emails when multimaster conflicts are detected.

5 Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

6 Restart the Model Repository Multimaster Component in all Opsware cores in the multimaster mesh.

See the *Opsware® SAS 5.2 Administration Guide* for information about the correct restart sequence for Opsware SAS components.

Configuring Email Notification Addresses for CDR

You can set up email notification addresses for the Opsware Code Deployment & Rollback feature. When users request that a service operation or synchronization be performed on their behalf, an email notification is sent to the individuals assigned to perform the requested service operation or synchronization.

Perform the following steps to configure email notification addresses for CDR. The Opsware Installer installs an Opsware core with placeholder values (EMAIL_ADDR) for these parameters. See "Code Deployment Setup" on page 349 in Chapter 12 for more information.

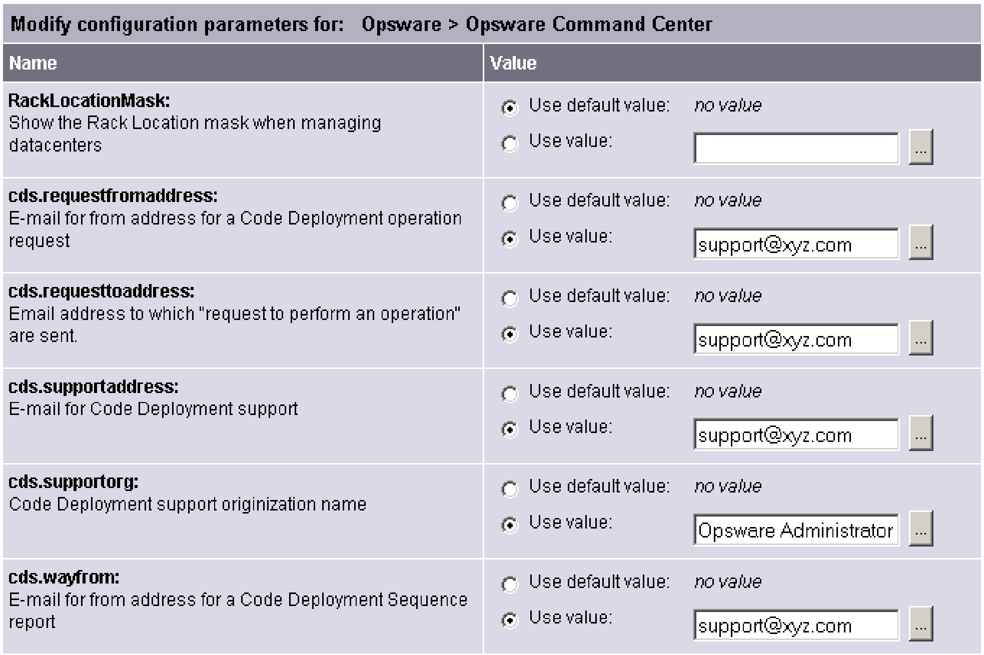
1. Login to the Opsware Command Center as the admin user with the password you supplied during the interview. Log in by opening a browser and entering the IP address of the server running the Opsware Command Center.

   The Opsware Command Center should be installed and listening. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Click the link for the Opsware Command Center. The configuration page for the Opsware Command Center appears, as Figure 2-2 shows.

Figure 2-2: CDR Email Notification Configuration Parameters



Modify configuration parameters for: Opsware > Opsware Command Center

Name	Value
RackLocationMask: Show the Rack Location mask when managing datacenters	● Use default value: *no value* ○ Use value:
cds.requestfromaddress: E-mail for from address for a Code Deployment operation request	○ Use default value: *no value* ● Use value: support@xyz.com
cds.requesttoaddress: Email address to which "request to perform an operation" are sent.	○ Use default value: *no value* ● Use value: support@xyz.com
cds.supportaddress: E-mail for Code Deployment support	○ Use default value: *no value* ● Use value: support@xyz.com
cds.supportorg: Code Deployment support originization name	○ Use default value: *no value* ● Use value: Opsware Administrator
cds.wayfrom: E-mail for from address for a Code Deployment Sequence report	○ Use default value: *no value* ● Use value: support@xyz.com

4. Customize the following parameters to include the following email notification information:

   - In the field **cds.requesttoaddress**, enter the email address to include in the “To:” field of the email message for a request notification.
   - In the field **cds.requestfromaddress**, enter the email address to include in the “From:” field of the email message for a request notification.
   - In the field **cds.wayfrom**, enter the email address to include in the “From:” field of the email message sent following completion of a sequence.
   - In the field **cds.supportaddress**, enter the email address to include for a facilities' support organization or contact person.
   - In the field **cds.supportorg**, enter the display name of a facilities' support organization.

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

6 Restart the Command Engine, Opsware Command Center, and the Model Repository Multimaster Component.

When you restart multiple Opsware SAS components, you must restart them in the correct order. See the *Opsware® SAS 5.2 Administration Guide* for information about the correct restart sequence for Opsware SAS components.

Chapter 3: User and Group Setup

IN THIS CHAPTER

This chapter discusses the following topics:

- Overview of Users, Groups, and Permissions
- Managing Users
- Managing User Groups and Permissions
- Managing the Special Administrators Group
- Using an External LDAP Directory Server with Opsware SAS
- Code Deployment Permissions

Overview of Users, Groups, and Permissions

Opsware SAS enforces a security policy that allows only authorized users to perform specific operations on specific servers. This chapter explains how to set up a role-based security structure for Opsware SAS. See *Planning Deployments for Opsware® SAS 5.2* for more information about security setup best practices.

Opsware Users

When you log in to the Opsware Command Center, you are prompted for an Opsware user name and password. Everyone in your organization who logs into the Opsware Command Center must have a unique Opsware user name and password. Every user should belong to one or more Opsware user groups. The tasks that a user is authorized to perform depend on the groups the user belongs to. You define permissions for a user group, not for individual users.

User names are stored in the Model Repository. You can create user names with the Opsware Command Center, or you can import them into the Model Repository from an external Lightweight Directory Access Protocol (LDAP) system.

Opsware User Groups and Permissions

A user group represents a role played by your organization's users. The permissions that you specify for a user group determine what the group's members can do with Opsware SAS. For example, Jane Doe could belong to the Advanced Users group, which has permission to run the OS Provisioning wizard.

The two types of permissions, resources and features, are explained in the following sections.

Resource Permissions

A resource is usually a set of managed servers or software nodes. A resource permission specifies if the users in a user group can view or modify a resource. The Opsware Command Center organizes resources into the following categories:

- **Customers**: The servers or software associated with a customer.
- **Facilities**: The servers associated with a facility.
- **Node Stack**: A subtree of the software tree (such as web servers) or service levels.
- **Server Groups**: The servers belonging to the specified public server group.

Each of these resource categories corresponds to a tab on the Edit Group page of the Opsware Command Center. (See Figure 3-2.) You can assign the following permissions to a resource:

- **Read**: This allows you to view the resource only.
- **Read & Write**: This allows you to view and change the resource.
- **None**: The resource does not appear in the Opsware Command Center and will not be displayed.

Access to a server depends on the server's association to a customer, association to a facility, and optionally, its membership in a public server group. For example, suppose that a server is associated with the Widget Inc. customer, resides in the Fresno facility, and belongs to the Accounting server group. To modify the server, the user group must have the permissions listed in Table 3-1. (The Read & Write permission for Accounting is required only if user group permissions are specified for public server groups.)

Table 3-1: Example of Resource Permissions

RESOURCE	GROUP PERMISSION
Customer: Widget, Inc.	Read & Write

Table 3-1: Example of Resource Permissions

RESOURCE	GROUP PERMISSION
Facility: Fresno	Read & Write
Server Group: Accounting	Read & Write

If the permissions for the customer, facility, or server group do not match, then the most restrictive permissions are enforced. For example, if the permission for the Customer is Read & Write, but the permission for the facility is Read, then the Read permission is enforced.

Managed servers and software nodes are the most common resources. Other types of resources are hardware definitions, realms, service levels, configurations, and templates.

Feature Permissions

The features described in this section are for the Features and Others tabs on the Edit Group page of the Opsware Command Center. (See Figure 3-5.) The Features tab lists the main tasks available in the Opsware Command Center; the Others tab lists sub-tasks.

An Opsware SAS feature is a task, such as running a script or uploading a patch. With feature permissions, you define the tasks that can be performed by the users of a group. In contrast with resource permissions, you specify the objects (software or servers) that can be modified or viewed with a feature.

To use a feature on a resource, the user must belong to a group that has the necessary permissions for both the feature and resource. For example, suppose that a server is associated with these resources: the Widget, Inc. customer and the Fresno facility. To install a patch on this server, the user must belong to a group with the permissions listed in Table 3-2.

Table 3-2: Example of Permissions Resources and Features

RESOURCE OR FEATURE	GROUP PERMISSION
Customer: Widget, Inc.	Read & Write
Facility: Fresno	Read & Write
Feature: Wizard Install Patch	Yes

Membership in Multiple Groups

If a user belongs to more than one user group, the user's permissions are the union of the permissions for the resources and features of the groups.

For example, Jane Doe belongs to both the Basic and Advanced groups, which have the permissions listed in Table 3-3. Because permissions are cumulative, Jane can perform the System Diagnosis task on the managed servers associated with the Widget Inc. customer.

Table 3-3: Example of Permissions and Multiple User Groups

RESOURCE OR FEATURE	BASIC GROUP PERMISSION	ADVANCED GROUP PERMISSION
Customer: Widget, Inc.	Read & Write	None
Customer: Acme Corp.	None	Read & Write
Feature: System Diagnosis	No	Yes

Restricted Views of the Opsware Command Center

The Opsware Command Center displays only those features and resources that the user's group has Read (or Read & Write) permissions.

For example, John Smith belongs to the Basic Users group, which has the permissions listed in Table 3-4. When John logs in, the Opsware Command Center displays only the servers for Widget Inc., but not those of Acme Corp. In the navigation panel of the Opsware Command Center, the Templates link appears, but not the Patches link.

Table 3-4: Example of Permissions and Restricted Views

RESOURCE OR FEATURE	BASIC GROUP PERMISSION
Customer: Widget, Inc.	Read & Write
Customer: Acme Corp.	None
Feature: Template	Yes
Feature: Patches	No

To locate or view a server, a user must belong to a group that has Read (or Read & Write) permission to both the customer and facility associated with the server. If the server also belongs to a server group with set permissions, then the user group must also have Read (or Read & Write) access to the server group. Otherwise, the user cannot locate the server in the Opsware Command Center.

Predefined User Groups

Opsware SAS includes the following predefined user groups:

- Basic Users
- Intermediate Users
- Advanced Users
- Opsware System Administrators

The Basic, Intermediate, and Advanced Users groups define roles for system administrators with increasing levels of responsibility. These system administrators perform operational tasks on managed servers and set up elements of Opsware SAS such as the Software Tree. The users in the Opsware System Administrators group manage Opsware SAS itself, performing tasks such as running the Opsware system diagnosis and multimaster tools.

Use of the predefined user groups is optional. You can change the permissions of the predefined user groups; you can also delete these groups. Changes or deletions of the predefined user groups are not affected by Opsware SAS upgrades.

See “Predefined User Group Permissions” on page 420 in Appendix for more information.

The Special Admin User and Administrators Group

The Opsware Installer creates a single user called `admin` in the Administrators group for the initial login to the Opsware Command Center. The password for `admin` is specified during the installation and should be changed immediately afterwards.

As a best practice, you should not add the `admin` user to other groups.

The users in the Administrators group manage the security structure of Opsware SAS. Members of the Administrators group create users and groups, specify permissions for groups, and assign users to groups. The Administrators group also has permissions to manage customers and facilities. Unlike the other groups in the Opsware Command Center, the Administrators group has its own tab and cannot be deleted. (See Figure 3-7.) Also, you cannot change the permissions of the Administrators group.

The Administrators group manages the security of Opsware SAS, whereas the Opsware System Administrators group manages the components and infrastructure of Opsware SAS.

Process Overview for Security Administration

The person responsible for the security of Opsware SAS creates and maintains users, groups, and permissions. This person must be able to log in to the Opsware Command Center as a user that belongs to the special Administrators group.

he following steps provide an overview of security administration for Opsware SAS:

1. Associate customers with managed servers. You may choose to use the initial customer that was specified during the installation of the Opsware core, or you may create new customers.

2. Create and name user groups to represent the roles of the people who will use the Opsware Command Center. Alternatively, you may use the predefined user groups.

3. Set the resource permissions for the user groups. (These permissions are on the Customers, Facilities, Node Stacks, and Server Groups tabs of the Edit Group page of the Opsware Command Center.) If using the predefined user groups, you may need to add permissions for the customers you created previously.

4. Set the feature permissions for the user groups. (These permissions are on the Features, Client Features, and Other tabs of the Opsware Command Center.)

5. Create new users or import existing users from an external LDAP.

6. Assign users to the appropriate groups.

Managing Users

To manage users, you must log in to the Opsware Command Center as a user that belongs to the Administrators group. The default member of the Administrators group is the `admin` user.

Creating a User

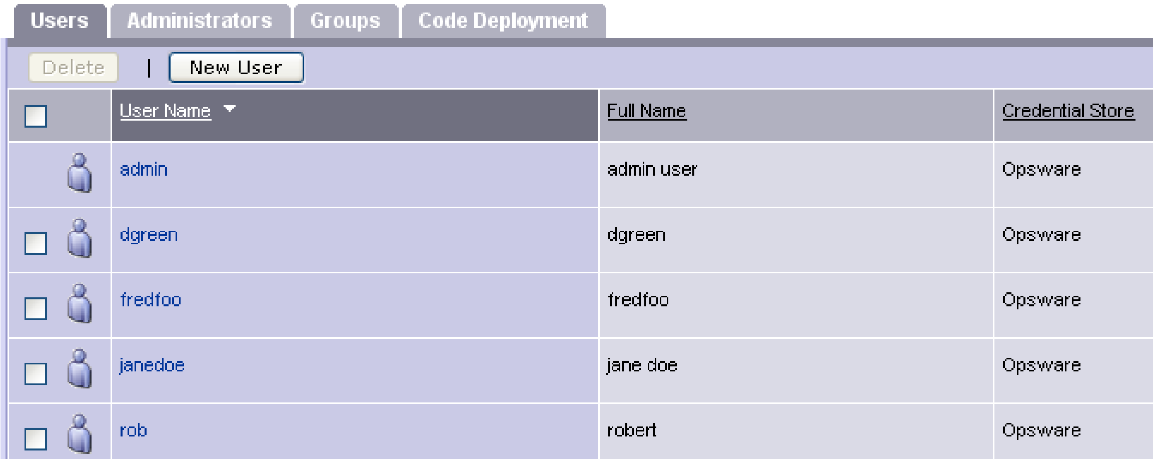
You can create Opsware users with the Opsware Command Center, or you can import users from an external LDAP directory. See "Using an External LDAP Directory Server with Opsware SAS" on page 52 in this chapter for more information.

To create a user with the Opsware Command Center, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.

    The Users tab appears. (See Figure 3-1.)

Figure 3-1: Users Tab



□		User Name ▼	Full Name	Credential Store
		admin	admin user	Opsware
□		dgreen	dgreen	Opsware
□		fredfoo	fredfoo	Opsware
□		janedoe	jane doe	Opsware
□		rob	robert	Opsware

2. Click the **New User** button.
3. On the Profile Editor page, fill in the required fields; they're labeled in bold font.

    The Login User Name may be different than the first, last, and full names. The Login User Name is not case sensitive and cannot be changed after the user is created.

    Optionally, you may assign the user to one or more of the groups listed at the bottom of the page. Or, you may change the user's group membership at a later time. If a user does not belong to a group, the user cannot view servers or perform tasks with the Opsware Command Center.
4. Click the **Save** button to create the user.

Editing User Information

Each Opsware user can edit the information for his or her own login user. To view or change information for your own login user, perform the following steps:

1. Click the My Profile link in the upper right corner of the Opsware Command Center.
2. When the My Profile page appears, you can change the full name, e-mail address, and other information. You cannot change the user name (login user) or permissions. If the user name has been imported from an external LDAP directory, then the password cannot be changed with the Opsware Command Center.

If your user belongs to the Administrators group, you may view or edit the information of any Opsware user. To do so, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Users tab, select an entry in the User Name column.
3. In the Profile Editor, modify the information as appropriate.
4. Click the **Save** button.

Viewing a User’s Permissions

You do not assign permissions directly to a user. Instead, you set the permissions on a user group and then assign a user to a group. To view the group membership and permissions of a user, follow the instructions in “Editing User Information” on page 33.

Deleting a User

When you delete a user, the user’s login and logout history is permanently stored, and the user is unassigned from user groups. After a user is deleted, you can create another user with the same name.

To delete an Opsware user, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Users tab, select the checkbox next to the user to be deleted.
3. Click the **Delete** button.

Managing User Groups and Permissions

To perform the tasks in this section, you must log in to the Opsware Command Center as a user (such as `admin`) that belongs to the Administrators group. If you change permissions while a user is logged in to the Opsware Command Center or OCC Client, the user must log out and log in again for the changes to take effect.

Creating a User Group

To create an Opsware user group, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Groups tab, click the **New Group** button.
3. On the New Group page, enter a role in the Group name field.
4. At this point, you can select the checkboxes under the Feature column to assign permissions to the group. The New Group page does not display all available permissions.
5. Click the **Save** button.

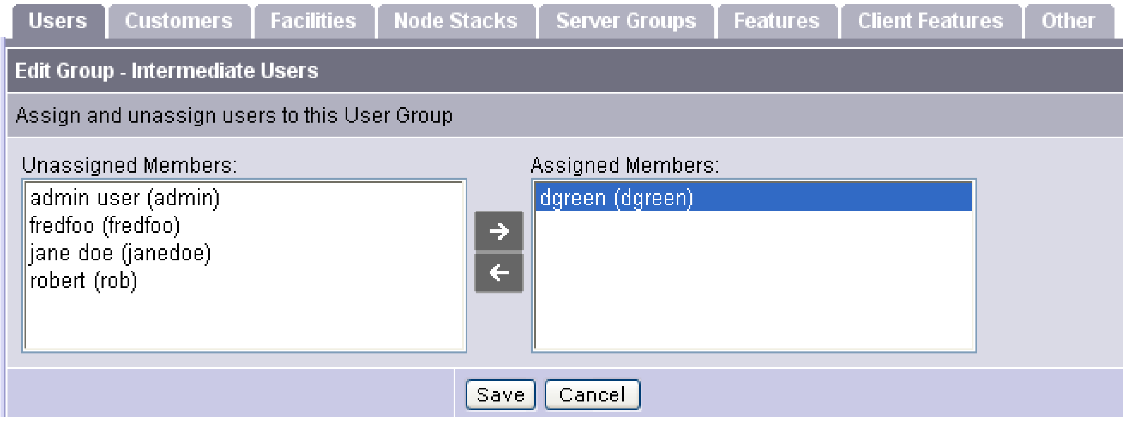
Assigning a User to a Group

You should assign each Opsware user to a group reflecting the user's role in your organization. If a user belongs to multiple user groups, the user has the permissions from all assigned groups. To assign an Opsware user to a user group, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Group tab, select a group from the Name column.

   The tabs shown in Figure 3-2 appear.

Figure 3-2: Tab for Assigning a User to a User Group



Edit Group - Intermediate Users

Assign and unassign users to this User Group

Unassigned Members:
admin user (admin)
fredfoo (fredfoo)
jane doe (janedoe)
robert (rob)

Assigned Members:
dgreen (dgreen)

3. In the Unassigned Members box, select the user name.
4. Click the right arrow.

5. To unassign a user, click the name in the Assigned Members box and click the left arrow.

6. Click the **Save** button.

Setting the Customer Permissions of a User Group

In Opsware SAS, you can associate a customer with a number of resources, including operating systems, packages, applications, templates, servers, service levels, hardware, and IP ranges. By setting the customer permission, you control the access that the users of a group have to the resources associated with the customer. For example, if you want the users of a group to be able to view (but not modify) the servers associated with the Widget Inc. customer, set the permission to Read. See “Opsware User Groups and Permissions” on page 28 in this chapter for more information.

The customer permissions also control access to the customer object itself. For example, to add a custom attribute to a customer, a user must belong to a group that has Read & Write permission to the specific customer, as well as permission for the Customers feature.

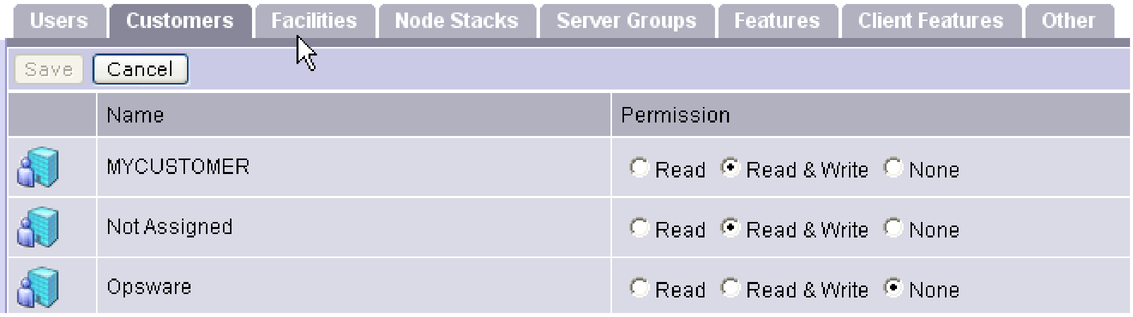
To control the access to the resources associated with a customer, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.

2. On the Groups tab, select an entry in the Name column.

   Another set of tabs appears, including the Customers tab. (See Figure 3-3.)

Figure 3-3: Customer Permissions Tab



	Name	Permission
	MYCUSTOMER	○ Read ● Read & Write ○ None
	Not Assigned	○ Read ● Read & Write ○ None
	Opsware	○ Read ○ Read & Write ● None

3. On the Customers tab, for each customer listed, select Read, Read & Write, or None.

4. Click the **Save** button.

Setting the Facility Permissions of a User Group

In Opsware SAS, a facility can be associated with resources such as servers and IP ranges. To modify a server of a particular facility, a user must belong to a group that has Read & Write permission for the facility. See “Opsware User Groups and Permissions” on page 28 in this chapter for more information.

The facility permissions also control access to the facility object itself. For example, to modify a property of a facility, a user must belong to a group that has Read & Write permission to the facility, as well as permission for the Facilities feature.

To control the access to the resources associated with a facility, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Groups tab, select an entry in the Name column. Another set of tabs appears, including the Facilities tab.
3. On the Facilities tab, select Read, Read & Write, or None.
4. Click the **Save** button.

Setting the Node Stack Permissions of a User Group

A node stack is a subtree in the Opsware software tree or a service level. Each subtree is a category of application software, such as Database Servers. To modify a node in the software tree, a user must belong to a group that has Read & Write permission for the stack containing the node. To view a node, a user must belong to a group that has Read permission on the stack.

For example, suppose that you want to allow Database Administrators (DBAs) to modify nodes in the Database Servers stack, but permit them to merely view the nodes in the other stacks. To implement this policy, you could create a DBA user group with Read & Write permission on the Database Servers stack, but with Read permissions on the other stacks. See “Opsware User Groups and Permissions” on page 28 in this chapter for more information.

To control access to a particular node stack, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Groups tab, select an entry in the Name column. Another set of tabs appears, including the Node Stacks tab. Select the Node Stacks tab.
3. For each node stack listed, select Read, Read & Write, or None.

4 Click the **Save** button.

Setting the Server Group Permissions of a User Group

To control access to the servers in a public server group, select a permission on the Server Groups tab. (You cannot control access to a private server group, which is visible only to the user who created it.)

If the Server Groups tab lists no server groups, then access to servers is not controlled by membership in server groups; however, access to servers is still controlled by their association with customers and facilities. If the Server Groups tab lists at least one server group, then access is denied to unlisted server groups (the equivalent of a None permission).

Access control based on server groups is optional. By default, membership in a server group does not restrict access. In contrast, for servers associated with customers or facilities, the default permission is None, which prohibits access.

You can combine customer, facility, and server group permissions to implement security policies. For example, you can restrict access to servers that are associated with the Acme Corp. customer, reside in the Fresno facility, and belong to a server group that contains only Windows servers.

A server group can contain other server groups. However, permissions are not inherited by the contained (children) server groups.

The permissions on the Server Groups tab control access to servers that belong to server groups. However, these permissions do not control the management of the server groups. To create, modify, or delete server groups, a user must belong to a user group that has the Manage Public Server Groups and the Model Public Server Groups checkboxes selected on the Other tab. Also, the Managed Servers and Groups checkbox must be selected on the Features tab.

To control access to servers that belong to a server group, perform the following steps:

1 From the navigation panel, select Administration ➤ Users & Groups.

2 On the Groups tab, select an entry in the Name column. Another set of tabs appears, including the Server Groups tab.

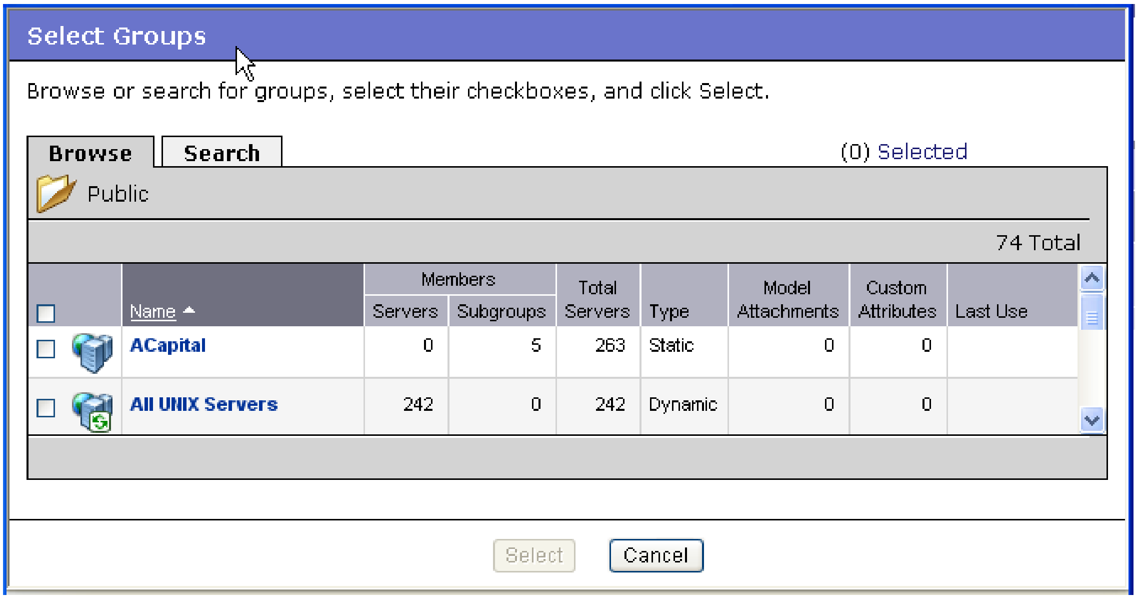
3 On the Server Groups tab, note the checkbox below the **Assign** button. If this checkbox is selected, then access to managed servers is not based on server groups.

4. Deselect the checkbox below the **Assign** button.

5. Click the **Assign** button.

   The Select Groups page appears. (See Figure 3-4.)

Figure 3-4: Select Server Groups Page



Select Groups

Browse or search for groups, select their checkboxes, and click Select.

□		Name ▲	Members		Total	Type	Model	Custom	Last Use
			Servers	Subgroups	Servers		Attachments	Attributes	
□		ACapital	0	5	263	Static	0	0	
□		All UNIX Servers	242	0	242	Dynamic	0	0	

6. On the Select Groups page, use the Browse or Search tab to locate the server groups.

7. On the Browser or Search tab, click on the server group name and then click the **Select** button.

8. On the Server Groups tab, for each server group listed, select the checkbox and select the button for the appropriate access.

   To allow viewing (but not modification) of the servers in a server group, select the Read permission. To allow both viewing and modification, select the Read & Write permission.

9. Click the **Save** button.

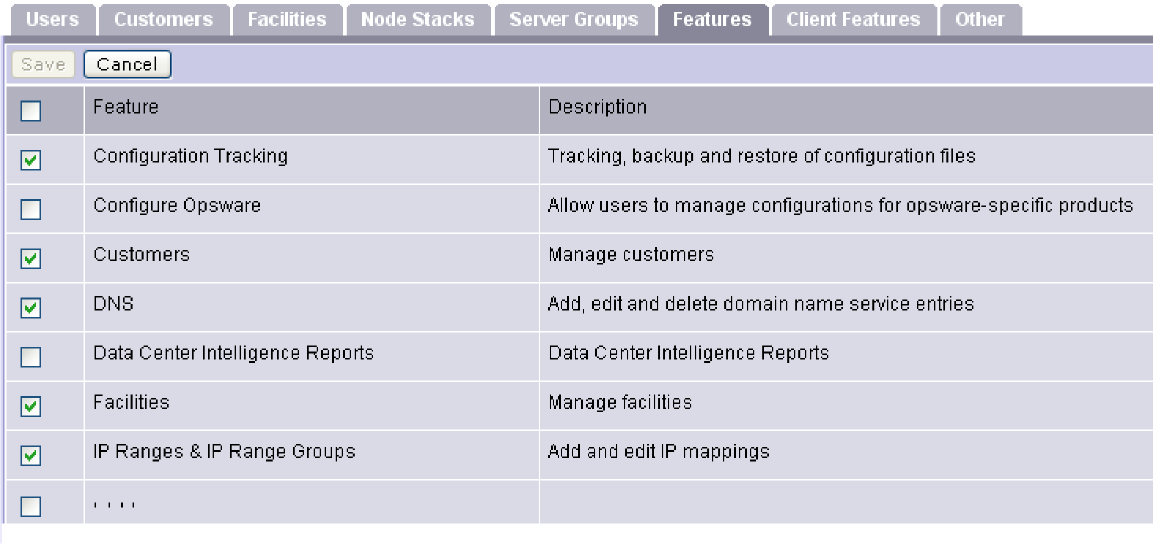
Setting the General Feature Permissions of a User Group

The Features tab of the Opsware Command Center includes many tasks, including managing the Opsware model and running the wizards. If the checkbox for a feature is unselected, then the Opsware Command Center does not display the related links in the navigation panel.

To allow the users in a group the ability to view and execute a task on the Features tab, perform the following:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Group tab, select a group from the Name column.
3. Another set of tabs appears, including the Features tab. (See Figure 3-5.)

Figure 3-5: Features Tab



☐	Feature	Description
☑	Configuration Tracking	Tracking, backup and restore of configuration files
☐	Configure Opsware	Allow users to manage configurations for opsware-specific products
☑	Customers	Manage customers
☑	DNS	Add, edit and delete domain name service entries
☐	Data Center Intelligence Reports	Data Center Intelligence Reports
☑	Facilities	Manage facilities
☑	IP Ranges & IP Range Groups	Add and edit IP mappings
☐	. . . .	

4. On the Features tab, select the checkbox for each feature that should be enabled for the user group. To prevent (and hide) a feature, deselect the checkbox.
5. Click the **Save** button.

Setting the OCC Client Features Permissions of a User Group

The Client Features tab of the Opsware Command Center lists permissions for the following features:

- Application Configuration
- Server Compliance

- Visual Packager
- Agent Deployment

To set these permissions for the OCC Client, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Group tab, select a group from the Name column. Another set of tabs appears, including the Client Features tab.
3. On the Client Features tab, select the appropriate permission buttons.
4. Click the **Save** button.

Setting the Other Features Permissions of a User Group

The Other tab of the Opsware Command Center contains the following permissions:

- **General Permissions**: Allows users in a user group to edit shared scripts or run “my scripts” as root. The Features tab also has script-related permissions: Scripts, and Wizard: Run Scripts.
- **Manage Servers Permissions**: Enables users in a user group to perform particular tasks on managed servers. The Allow Run Refresh Jobs permission lets users specify a job to update the servers list. The Manage Public Servers Group permission enables users to create server groups, modify the group properties, and change the group membership (through rule changes, or adding and deleting servers). All users may view all public server groups. The Model Public Servers Group permission lets users add or remove model attachments, including patches, applications, service levels, and custom attributes. (These permissions apply to public, not private server groups. Only the user who creates a private server group can view or modify it.) The Features tab also has a permission related to managing servers: Managed Servers and Groups.
- **Locking Permissions**: Determines whether the users in a user group can lock nodes of a particular type in the software tree, or edit locked nodes. (To lock a node, the users must belong to a group that also has Read & Write access to the corresponding stack, as specified on the Node Stacks tab.) For example, you may want to permit only DBAs to lock the nodes under Database Servers. The DBAs would be able to lock a node (such as Oracle Server 9) on the Edit Node page, prohibiting users in other groups from adding packages to the node. The users in the other groups cannot modify the node, but can view and install the node’s application onto managed servers.

To set the permissions on the Other tab, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. On the Group tab, select a group from the Name column. Another set of tabs appears, including the Other tab.
3. On the Other tab, select the checkboxes to assign permissions to this user group.
4. Click the **Save** button.

Setting the Permissions for the Opsware Global Shell Feature

To set up permissions for the Opsware Global Shell feature, perform the following steps:

1. Log in to the Opsware Command Center as a user that belongs to the Administrators group.
2. Launch the OCC Client.
3. Open a Global Shell Session.
4. Run the `aaa` command-line utility to specify the operations that can be performed within a Global Shell Session by the members of a user group.

The `aaa` utility is available only within a Global Shell Session. The sections that follow describe Global Shell permissions and the `aaa` utility. See the *Opsware® SAS 5.2 User's Guide* for more information about the Global Shell feature.

Global Shell Permissions

Permissions identify the operations you can perform on a managed server. These operations are specified with the `aaa` utility. Most of these operations, such as loginToServer, can be granted on both managed servers and on a login basis. However, the relayRdpToServer operation is granted on managed servers, but not on a login. Table 3-5 identifies and describes the server operations in Global Shell. In the table, the On Server column identifies which operations can be granted for managed servers, and the On Login column identifies the operations that can be granted on a login basis.

Table 3-5: Global Shell Operations

OPERATION	DESCRIPTION	ON SERVER	ON LOGIN
launchGlobalShell	Launches the Global Shell.	No	No

Table 3-5: Global Shell Operations (continued)

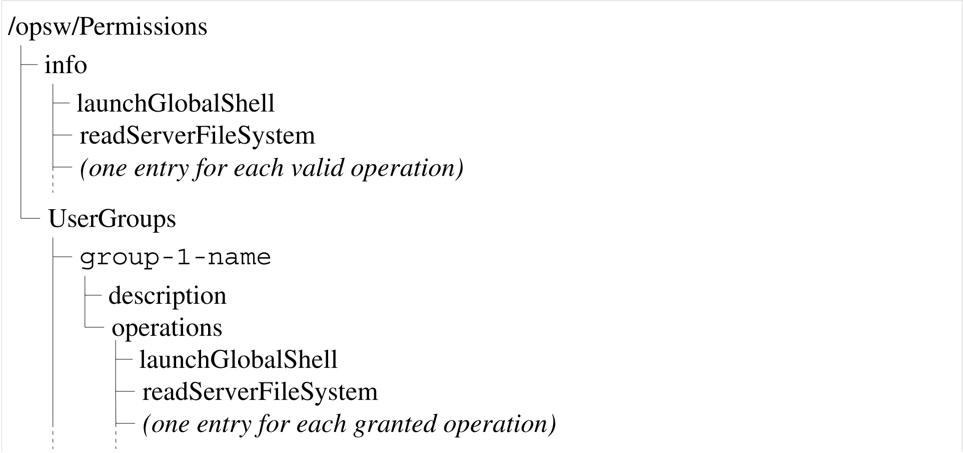
OPERATION	DESCRIPTION	ON SERVER	ON LOGIN
loginToServer	Opens a shell session on a Unix server. In the OCC Client, this is the Remote Terminal feature that opens a terminal window for a Unix server.	Yes	Yes
readServerFilesystem	Reads a managed server as a specific login. In the OCC Client, use the Server Explorer to browse the file system of a managed server.	Yes	Yes
readServerRegistry	Reads registry files as a specific login. In the OCC Client, use the Server Explorer to view the Windows Registry.	Yes	Yes
relayRdpToServer	Opens an RDP session on a Windows server. In the OCC Client, this is the Remote Terminal feature that opens an RDP client window for a Windows server.	Yes	No
runCommandOnServer	Runs a command or script on a managed server using a `rosh` operation, where that command or script already exist. In the OCC Client, this is used for Windows Services when you use the Server Explorer.	Yes	Yes
runTrustedOnServer	Runs a shared saved script (which is stored in `/opsw/Script/Shared`) on a managed server.	Yes	Yes
writeServerFilesystem	Modifies files on a managed server as a specific login. In the OCC Client, use the Server Explorer to modify the file system of a managed server.	Yes	Yes

A login is not specific to a particular operating system. For example, if the permissions specify that a user can read the file system as root, then root will appear under the files subdirectory, regardless of the operating system. The Server Explorer of the OCC Client displays the login names that you have been authorized to access that server's file system. Examples of these login names are Administrator, root, and LocalSystem.

Permissions Directory

The `Permissions` directory contains information about the Global Shell permissions that have been granted for your Opsware SAS. Figure 3-6 illustrates the structure of the `Permissions` directory.

Figure 3-6: Permissions Directory



```
/opsw/Permissions
 ├ info
 │  ├ launchGlobalShell
 │  ├ readServerFileSystem
 │  ├ (one entry for each valid operation)
 │  ┆
 └ UserGroups
    ├ group-1-name
    │  ├ description
    │  └ operations
    │     ├ launchGlobalShell
    │     ├ readServerFileSystem
    │     ├ (one entry for each granted operation)
    ┆     ┆
```

This directory contains the following two subdirectories:

- The `info` subdirectory contains a file for each of the operations to which permission can be granted. See Table 3-5 for a list of operations.
- The `UserGroups` subdirectory contains a subdirectory for each user group that is defined in your Opsware SAS.

  Each user group directory contains a `description` file and an `operations` directory. The `description` text file is a brief description of the user group (as it was entered in the OCC). The `operations` directory contains a text file for each operation to which the user group has been granted some type of permission. Each text file summarizes the parameters of the permissions for that operation and user group.

  For example, the `readServerFilesystem` text file is in the `operations` directory for the `Advanced Users` group:

```
/opsw/Permissions/UserGroups/Advanced Users/operations/
readServerFilesystem
```

The `readServerFilesystem` text file contains the following information:

```
Facility: C40(40) Login: sysadmin
Group: Unix Servers (2880040) Login: root
```

In this example, all members of the `Advanced Users` group can read the file system as user `sysadmin` on servers that belong to `Facility C40` (with ID `40`), and as user `root` on servers that belong to the server group `Unix Servers` (with ID `2880040`).

If there is no text file for an operation, the user group does not have permission to perform that operation. If there is an empty text file for an operation, the user group has permission to perform the operation, but the operation does not have any parameters. The launchGlobalShell operation does not have any parameters. See Table 3-5.

The aaa Utility

The `aaa` utility of the Global Shell grants and revokes permissions for operations on a managed server. These permissions are stored in the `/opsw/Permissions` directory of the OGFS. See “Permissions Directory” on page 44 in this chapter for more information.

The `aaa` utility has the following syntax:

```
aaa <command> <subcommand> [options]
```

The following values are valid in the `aaa` utility syntax:

- `<command>` is `shell-perm`
- `<subcommand>` is either `grant` or `revoke`
- One or more `[options]` can be specified.

The following is the syntax for granting permissions:

```
aaa shell-perm grant -o <operation> [-u <user-group>]
   [-f <facility> | -c <customer> | -g <server-group>
   [-l <login>]]
```

The following list describes each option:

`-o` The operation on which to grant permission. This is a required option.

`-u` The user group that is assigned the permission.

This value is inferred from the current working directory if it corresponds to a user group. If it cannot be inferred, you must specify a user group.

`-f` The name, ID, or path to a facility, such as:

```
/opsw/Facility/Chicago
```

Permission will be granted to all servers in this facility.

`-c` The name, ID, or path to a customer, such as:

```
/opsw/Customer/Alpha
```

Permission will be granted to all servers that belong to this customer.

`-g` The name, ID, or path to a server group, such as:

```
/opsw/Group/Public/Unix Servers
```

Permission will be granted to all servers that belong to this group. To specify the server group by name, omit `/opsw/Group/`. Only public server groups should be used.

`-l` A login account that exists on the servers that are specified by the `-f`, `-c`, or `-g` option.

✔ For operations that are performed on a server, one of the `-f`, `-c`, or `-g` options is required.

The following example gives all members of the `Advanced Users` group permission to launch the Global Shell feature:

```
aaa shell-perm grant -o launchGlobalShell -u ‘Advanced
Users’
```

The following example gives all members of the `Unix Admin` user group permission to log in to all servers that are in the `Public/Unix Servers` server group as `root`:

```
aaa shell-perm grant -o loginToServer -u ‘Unix Admin’
  -g ‘Public/Unix Servers’ -l root
```

As a best practice, when you are granting permissions, use care when you select servers so that you do not capture more servers than you intend. This is particularly important when using the `-c` or `-f` option. For example, if you want to grant permission to the loginToServer operation for all servers in the `Chicago` facility as `root`, you could use the `-f` option to select all servers in a particular facility. However, this may also select Windows servers, which is probably not desired since the `root` user does not typically exist on Windows servers. In this case, you should define a public server group that only includes servers in the `Chicago` facility which are running a Unix operating system.

The `-f` and `-c` options are provided as a convenience; however, in general, it is recommended that you define permissions based on server groups instead. See the *Opsware® SAS 5.2 User's Guide* for more information about server groups.

The following is a syntax example that revokes permissions:

```
aaa shell-perm revoke -o <operation> [-u <user-group>]
    [-f <facility> | -c <customer> | -g <group>]
    [-l <login>]
```

The following example removes the permission for the `Unix Admin` user group to log in to servers that belong to the `Public/Unix Servers` server group (for any login, since the `-l` option is not specified):

```
aaa shell-perm revoke -o loginToServer -u 'Unix Admin'
   -g 'Public/Unix Servers'
```

It is assumed that this permission was previously granted to the `Unix Admin` user group. The `revoke` command can only remove a permission that was previously granted. If the permission was not previously granted, this command has no effect.

The `revoke` command will only remove a permission for a specific user group. If a user has overlapping permissions, revoking permissions from a single user group will not prevent the user from performing that operation. For example, suppose a user belongs to two user groups and both have permission to the launchGlobalShell operation. If this permission is revoked from only one of those user groups, the user will still have permission to the launchGlobalShell operation.

Managing the Special Administrators Group

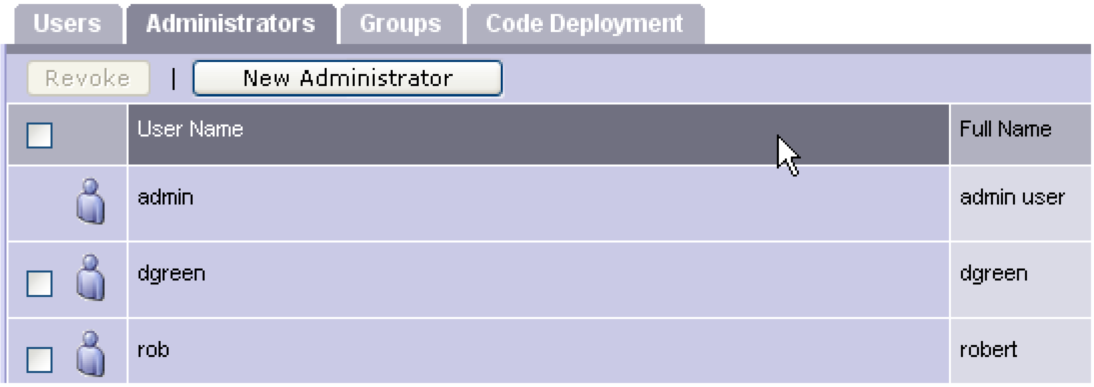
To manage the Administrators group, users must belong to the Administrators group. Only those users who belong to the Administrators group can manage Opsware SAS users and user groups. You can change user membership of the Administrators group, but you cannot modify the group in any other way. See “The Special Admin User and Administrators Group” on page 31 in this chapter for more information.

Adding a User to the Administrators Group

To add a user to the Administrators group, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. Select the Administrators tab. (See Figure 3-7.)

Figure 3-7: Administrators Tab



☐	User Name	Full Name
	admin	admin user
☐	dgreen	dgreen
☐	rob	robert

3. Click the **New Administrator** button.
4. On the Add Administrators page, select the user you want to add to the Administrators group.
5. Click the **Save** button.

Removing a User from the Administrators Group

To remove a user from the Administrators group, perform the following steps:

1. From the navigation panel, select Administration ➤ Users & Groups.
2. Select the Administrators tab.
3. Select the checkbox for the user.
4. Click the **Revoke** button.

Overview of Password Policy Parameters

The Opsware administrator can enable and configure the password policy parameters for accessing the Opsware Command Center. The passwords will be checked against the configured parameters when user accounts are created by the Opsware administrator or when the passwords are changed by the users or the administrator. The users, including the administrators will be alerted with an error message if their password does not match the criteria specified in the configured password policy parameters.

The Opsware administrator can use the Administration features of the Opsware Command Center to enable and configure the following parameters in a password:

- Set the maximum number of consecutive repeating characters allowed for a password. By default the value is 2, and the value cannot be 0.
- Set the minimum character limit required for a password. By default the minimum character limit is 6 and the maximum character limit is 50.
- Set the minimum non-alphabetic character limit required for a password. By default the minimum non-alphabetic character limit is 0 and the value cannot be greater than the value specified for the minimum character limit required for a password.

The Opsware administrator can configure any number of the three password policy parameters for accessing the Opsware Command Center. If the password policy parameter is disabled the password will be checked to ensure that it has at least 6 characters.

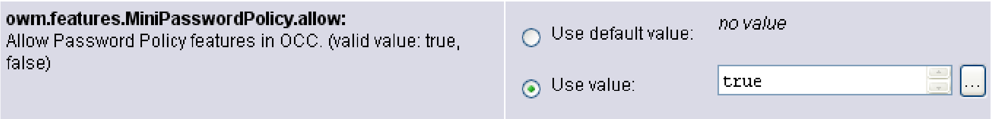
Enabling and Configuring Password Policy Parameters

Perform the following steps to enable and configure the password policy parameters for accessing the Opsware Command Center.

1. Log in to the Opsware Command Center as an user with admin privileges with the password you supplied during the interview. The Opsware Command Center home page appears.
2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.
3. Under Select a Product, click the Opsware Command Center link. The Modify Configuration Parameters for the Opsware Command Center page appears.

4 To enable the password policy parameters, in the field **owm.features.MiniPasswordPolicy.allow**, enter `true` as Figure 3-8 shows.The default value is false.

Figure 3-8: Enabling Password Policy Parameters



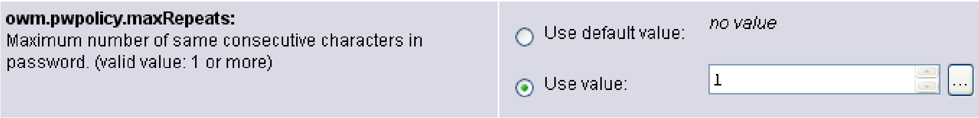
owm.features.MiniPasswordPolicy.allow:
Allow Password Policy features in OCC. (valid value: true, false)

○ Use default value: *no value*

● Use value: true

5 In the field **owm.pwpolicy.maxRepeats**, enter a value specifying the maximum number of consecutive repeating characters allowed for a password. The value entered must be greater than 0; the default value is 2. See Figure 3-9.

Figure 3-9: Configuring Maximum Number of Repeating Characters for a Password



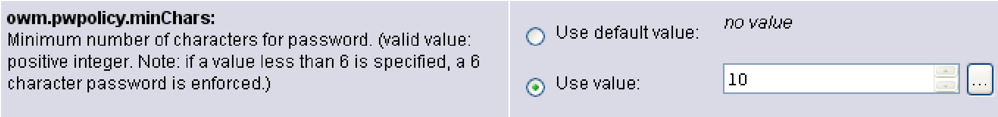
owm.pwpolicy.maxRepeats:
Maximum number of same consecutive characters in password. (valid value: 1 or more)

○ Use default value: *no value*

● Use value: 1

6 In the field **owm.pwpolicy.minChars**, enter a value specifying the minimum number of characters required for a password. The value must be a positive integer; the default value is 6. See Figure 3-10.

Figure 3-10: Configuring Minimum Number of Characters for a Password



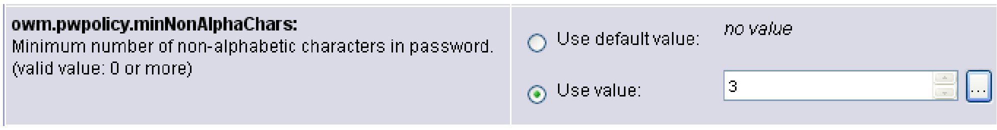
owm.pwpolicy.minChars:
Minimum number of characters for password. (valid value: positive integer. Note: if a value less than 6 is specified, a 6 character password is enforced.)

○ Use default value: *no value*

● Use value: 10

7 In the field **owm.pwpolicy.minNonAlphaChars**, enter a value specifying the minimum number of non-alphabetic characters required for a password. The value cannot be greater than the value specified for the minimum character limit; the default value is 0. See Figure 3-11.

Figure 3-11: Configuring Non-alphabetic Characters for a Password



owm.pwpolicy.minNonAlphaChars:
Minimum number of non-alphabetic characters in password. (valid value: 0 or more)

○ Use default value: *no value*

● Use value: 3

8. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

When you make changes to the password policy System Configuration settings in one core of a mesh, the change is reflected in that core only. The changes get propagated to other cores in a mesh only after you restart the other cores.

Disabling Password Policy Parameters

Perform the following steps to disable the password policy parameters for accessing the Opsware Command Center.

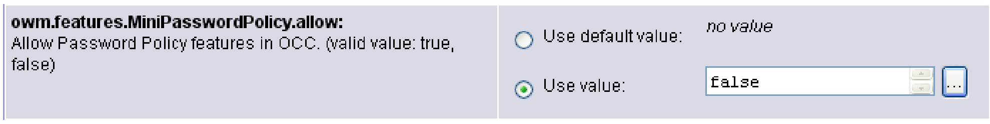
1. Log in to the Opsware Command Center as an user with admin privileges with the password you supplied during the interview. The Opsware Command Center home page appears.

2. From the navigation panel, click System Configuration under Administration. The Select a Product page appears.

3. Under Select a Product, click the Opsware Command Center link. The Modify Configuration Parameters for the Opsware Command Center page appears.

4. To disable the password policy parameters, in the field **owm.features.MiniPasswordPolicy.allow**, select the default value (`false`) as Figure 3-12 shows. If you select the default value, the password will be checked to ensure that it has at least 6 characters.

Figure 3-12: Disabling Password Policy Parameters



owm.features.MiniPasswordPolicy.allow:
Allow Password Policy features in OCC. (valid value: true, false)

○ Use default value: *no value*

● Use value: false

5. Click Save to apply the changes. The configuration page refreshes and a message appears that the update was successful.

When you make changes to the password policy System Configuration settings in one core of a mesh, the change is reflected in that core only. The changes get propagated to other cores in a mesh only after you restart the other cores.

Using an External LDAP Directory Server with Opsware SAS

You can configure Opsware SAS to use an external LDAP directory service for user authentication. With external authentication, you do not have to maintain separate user names and passwords for Opsware SAS. When users log in to the Opsware Command Center, they enter their LDAP user names and passwords.

Imported Users

With the Opsware Command Center, you search for users in the external LDAP and then you import selected users into Opsware SAS. You can limit the search results by specifying a filter. The import process fetches the following user attributes from the LDAP:

```
firstName
lastName
fullName
emailAddress
phoneNumber
street
city
state
country
```

After the import process, you may edit the preceeding list of attributes with the Opsware Command Center. However, you cannot change the user login name or password with the Opsware Command Center. Importing a user is a one-time, one-way process. Changes to the user attributes you make using the Opsware Command Center are not propagated back to the external LDAP directory server, and vice versa.

Imported users are managed in the same way as users created by the Opsware Command Center. For example, you use the Opsware Command center to assign imported users to user groups and to delete imported users from Opsware SAS. If you delete an imported user with the Opsware Command Center, the user is not deleted from the external LDAP directory.

If you use external authentication, you can still create separate users with the Opsware Command Center. However, this practice is not recommended. On the User tab of the Opsware Command Center, the Credential Store column identifies the source (External or Opsware) of each user.

SSL and External Authentication

Although SSL is not required for external authentication, it is strongly recommended. The certificate files needed for LDAP over SSL must be in Privacy Enhanced Mail (PEM) format. Depending on the LDAP server, you may need to convert the server's CA certificate to PEM format.

Supported External LDAP Directory Servers

The following directory server products may be used with Opsware SAS:

- Microsoft Active Directory (Windows 2000 or Windows 2003)
- Novel eDirectory 8.7
- SunDS 5.2

Overview of Process for Using an External LDAP

To use an LDAP directory server with Opsware SAS, perform the following basic steps:

1. Add the `aaa.ldap` entries to the `twist.conf` file with a text editor. See "Modifying the Web Services Data Access Engine Configuration File" on page 53.
2. Get the SSL server certificate from the LDAP directory server. See "Importing Server Certificate from External LDAP into Opsware SAS" on page 57. (Use of SSL is not required, but strongly recommended.)
3. Edit the loginModule.conf file with a text editor. See "Configuring the JAAS Login Module (loginModule.conf)" on page 58.
4. Restart the Web Services Data Access Engine:
   ```
   /etc/init.d/twist stop
   /etc/init.d/twist start
   ```
5. Use the Opsware Command Center to import users from the LDAP directory server into Opsware SAS. See "Importing External LDAP Users" on page 59.

In a mulitmaster mesh, you must perform steps 1 - 4 on each Web Services Data Access Engine.

Modifying the Web Services Data Access Engine Configuration File

To modify `twist.conf`, perform the following steps:

1. Log in as root to the system running the Web Services Data Access Engine, an Opsware core component.

2 In a text editor, open this file:
`/cust/twist/etc/twist.conf`

3 In the text editor, add the necessary properties (listed in Table 3-6) to the `twist.conf` file. Although not required, the SSL properties are recommended. For examples of the lines required for the `twist.conf` file see, the sections that follow Table 3-6.

4 Save the `twist.conf` file and exit the text editor.

Table 3-6: Properties in twist.conf for an External LDAP

PROPERTY	DESCRIPTION
`aaa.ldap.hostname`	The hostname of the system running the LDAP directory server.
`aaa.ldap.port`	The port number of the LDAP directory server.
`aaa.ldap.search.binddn`	The BIND DN (Distinguished Name) for LDAP is required by the search of the import user operation. A blank value denotes an anonymous BIND.
`aaa.ldap.search.pw`	The BIND password for LDAP is required by the search for the import user operation. A blank value denotes an anonymous BIND.
`aaa.ldap.search.filter.template`	The search filter template is used, with optional filter substitution, as the filter in the LDAP search for the user import. Any dollar sign ($) character in the template will be replaced by the filter string specified in the Import Users page of the Opsware Command Center. (The default value is an asterisk (*) which matches all entries.)
`aaa.ldap.search.base.template`	The configurable template allows support for a range of DIT configurations and schema in the LDAP service. The search base template string is used for the “search base” in the LDAP search operations for the user import.

Table 3-6: Properties in twist.conf for an External LDAP

PROPERTY	DESCRIPTION
`aaa.ldap.search.naming.attribute`	The naming attribute allows support for a range of schema in the LDAP services. Some use `uid`, others use `cn`, and so on. The value of this attribute is used for the internal user ID in Opsware SAS.
`aaa.ldap.search.naming.display.name`	The naming attribute allows support for a range of schema in the LDAP services. Some use `cn`, others use `displayName`, and so on. The value of this attribute is used for the Full Name of Opsware SAS user.
`aaa.ldap.ssl`	SSL: A value of true enables SSL.
`aaa.ldap.secureport`	SSL: The secure port of the LDAP directory server.
`aaa.ldap.usestarttls`	SSL: A value of true enables `Start TLS`.
`aaa.ldap.servercert.ca.fname`	SSL: The fully qualified file name of the server CA certificate.
`aaa.ldap.clientcert`	SSL: A value of true enables client certificate use.
`aaa.ldap.clientcert.fname`	SSL: The fully qualified file name of the client certificate.
`aaa.ldap.clientcert.ca.fname`	SSL: The fully qualified file name of the client CA certificate.

Example twist.conf for Microsoft Active Directory Without SSL

```
aaa.ldap.search.binddn=cn=Administrator,cn=users,dc=example,dc=
com
aaa.ldap.search.pw=secret
aaa.ldap.hostname=myservername.internal.example.com
aaa.ldap.port=389
aaa.ldap.search.filter.template=(&(objectclass=user)(cn=$))
aaa.ldap.search.base.template=cn=users,dc=example,dc=com
aaa.ldap.search.naming.attribute=samaccountname
aaa.ldap.search.naming.display.name=cn
```

Example twist.conf for Microsoft Active Directory With SSL

```
aaa.ldap.search.binddn=cn=Administrator,cn=users,dc=example,dc=
com
aaa.ldap.search.pw=secret
aaa.ldap.hostname=myservername.internal.example.com
aaa.ldap.secureport=636
aaa.ldap.ssl=true
aaa.ldap.ssl.servercert.ca.fname=/var/lc/crypto/twist/cert.pem
aaa.ldap.search.filter.template=(&(objectclass=user)(cn=$))
aaa.ldap.search.base.template=cn=users,dc=example,dc=com
aaa.ldap.search.naming.attribute=samaccountname
aaa.ldap.search.naming.display.name=cn
```

Example twist.conf for Novell eDirectory Without SSL

```
aaa.ldap.search.binddn=cn=admin,o=example
aaa.ldap.search.pw=secret
aaa.ldap.hostname=myservername.internal.example.com
aaa.ldap.port=389
aaa.ldap.search.filter.template=(&(objectclass=inetorgperson)(u
id=$))
aaa.ldap.search.base.template=o=example
aaa.ldap.search.naming.attribute=uid
aaa.ldap.search.naming.display.name=cn
```

Example twist.conf for Novell eDirectory Without SSL

```
aaa.ldap.search.binddn=cn=admin,o=example
aaa.ldap.search.pw=secret
aaa.ldap.hostname=myservername.internal.example.com
aaa.ldap.secureport=636
aaa.ldap.ssl=true
aaa.ldap.ssl.servercert.ca.fname=/var/lc/crypto/twist/
ldapcert.pem
aaa.ldap.search.filter.template=(&(objectclass=inetorgperson)(u
id=$))
aaa.ldap.search.base.template=o=example
aaa.ldap.search.naming.attribute=uid
aaa.ldap.search.naming.display.name=cn
```

Example twist.conf for SunDS Without SSL

```
aaa.ldap.search.binddn=cn=Directory Manager
aaa.ldap.search.pw=secret
aaa.ldap.hostname=myservername.internal.example.com
aaa.ldap.port=389
aaa.ldap.search.filter.template=(&(objectclass=inetorgperson)(u
id=$))
aaa.ldap.search.base.template=ou=people,dc=example,dc=com
aaa.ldap.search.naming.attribute=uid
aaa.ldap.search.naming.display.name=cn
```

Example twist.conf for SunDS With SSL

```
aaa.ldap.search.binddn=cn=Directory Manager
aaa.ldap.search.pw=secret
aaa.ldap.hostname=myservername.internal.example.com
aaa.ldap.secureport=636
aaa.ldap.ssl=true
aaa.ldap.ssl.servercert.ca.fname=/var/lc/crypto/twist/
ldapcert.pem
aaa.ldap.search.filter.template=(&(objectclass=inetorgperson)(u
id=$))
aaa.ldap.search.base.template=ou=people,dc=example,dc=com
aaa.ldap.search.naming.attribute=uid
aaa.ldap.search.naming.display.name=cn
```

Importing Server Certificate from External LDAP into Opsware SAS

For SSL, the necessary certificates must be extracted from the LDAP and copied over to Opsware SAS.

To import a server certificate from the LDAP into Opsware SAS, perform the following steps:

1. Extract the server certificate from the external LDAP. For instructions, see the following sections.

2. Convert the extracted certificate to PEM format.

   Certificates created on Windows systems are in Distinguished Encoding Rules (DER) format. The following example converts a certificate from DER to PEM format with the `openssl` utility:

   ```
   OpenSSL> x509 -inform DER -outform PEM -in mycert.der \
   -out mycert.pem
   ```

3. Copy the server certificate to the location specified by the Web Services Data Access Engine configuration file (`twist.conf`). For example, the `twist.conf` file could have the following line:

   ```
   aaa.ldap.ssl.servercert.ca.fname=/var/lc/crypto/twist/
   ldapcert.pem
   ```

Extracting the Server Certificate from Microsoft Active Directory

To extract the server certificate, perform the following steps:

1. Run either the Certificates MMC snap-in console or the Certificate Services web interface.
2. Export the Root CA cert from the Windows CA into DER format.

Extracting the Server Certificate from Novell eDirectory

To extract the server certificate, perform the following steps:

1. Find out the name of the local CA entry. (Example: CN=CORP-TREE CA.CN=Security)
2. Open the eDirectory Administration utility and click Modify Object.
3. Enter the entry name (CN=CORP-TREE CA.CN=Security).
4. Select the Certificates tab.
5. Click Self Signed Certificate.
6. Click Export.
7. In the dialog, click No for exporting the private key and then click Next.
8. Select the appropriate format (usually DER).
9. Click **Save the exported certificate to a file**.

Extracting the Server Certificate from SunDS

Typically, instead of exporting a server CA certificate from SunDS, you obtain the certificate that was imported into SunDS.

Configuring the JAAS Login Module (loginModule.conf)

To configure the JAAS login module, perform the following steps:

1. Log in as root to the system running the Web Services Data Access Engine, an Opsware core component.
2. In a text editor, open this file:
   `/cust/twist/etc/loginModule.conf`
3. In the text editor, modify the `loginModule.conf` file so that it contains the following lines:

```
/** Login configuration for JAAS modules **/
```

```
TruthLoginModule {
  com.opsware.login.TruthLoginModule sufficient debug=true;
  com.opsware.login.LdapLoginModule sufficient debug=true;
};
```

4 Save the `loginModule.conf` file and exit the text editor.

Importing External LDAP Users

Before importing external LDAP users, you must complete the prerequisite steps. See "Overview of Process for Using an External LDAP" on page 53 in this chapter for more information. After you import the users, the users may log in to the Opsware Command Center with their LDAP user names and passwords.

To import external users, perform the following steps:

1 In the Opsware Command Center, from the navigation panel, select Administration ➤ Users & Groups.

2 Select the Users tab. The page lists the existing Opsware SAS users.

3 On the Users tab, click the **Import External Users** button.

The page displays the users in the LDAP that match the search filter. The default filter is an asterisk (*), indicating that all users are selected. If a checkbox does not appear to the left of the user name, then the user already exists in Opsware SAS and cannot be imported.

If Opsware SAS cannot connect to the LDAP, check for error messages in the following file:

```
/var/lc/twist/stdout.log
```

4 To change the search filter, enter a value in the field to the left of the **Change Filter** button. For example, to fetch only those user names beginning with the letter A, you enter A* in the field.

5 If you modified the search filter in the preceding step, click the **Change Filter** button. The page displays the users in the LDAP that match the search filter.

6 You can assign users to the user groups listed at the bottom of the page or you can assign them later.

7 Select the checkboxes for the users you want to import. To import all users displayed, select the top checkbox.

8 On the Import Users page, click the **Import** button.

Code Deployment Permissions

Permissions to perform CDR operations are based on user membership in user groups predefined specifically for CDR. Users must also have the necessary permissions for the customer associated with the servers. Except for the Super User group, CDR operations are customer specific. A member of the Super User group can perform CDR operations on the servers of any customer.

The Opsware Command Center might still show the legacy term CDS. However, all documentation references use Opsware SAS Code Deployment & Rollback term CDR.

The Opsware Command Center includes predefined user groups that have specific permissions to perform CDR operations. Opsware administrators create and add users to these user groups to grant them permissions to perform specific CDR operations, based on their role in an organization. When logged into the Opsware Command Center, users see only the services, synchronizations, and sequences that they have authorization to perform because of their user group membership. Users are assigned to these groups as part of the Create User process.

See “Code Deployment User Groups” on page 424 in Appendix for more information.

See “Overview of Code Deployment & Rollback Setup” on page 356 in Chapter 12 for more information about the process to deploy code and content to managed servers.

When a user requests a service operation, synchronization, or sequence, an e-mail notification is sent to the individuals assigned to actually perform the requested service operation or synchronization.

Adding Members to a Code Deployment User Group

Permissions to perform specific Code Deployment operations are granted based on a user's membership in specific Code Deployment user groups.

1. From the navigation panel, select Administration ➤ Users & Groups. The Manage Users: View Users page appears.

2. Select the Code Deployment tab.

3. Select the code deployment user group that you want to modify by clicking the hyperlinked user group name.

   The Users and Groups: Edit Code Deployment Group - [group name] page appears.

4. From the drop-down list, choose the customer whose group membership you want to modify.

Code Deployment permission is assigned based on an Opsware customer. You cannot select Customer Independent, Not assigned, and Opsware customers and modify their group membership.

5. To add a user to the group, select the name in the left box, and then click the right arrow.

6. Click the **Save** button when you finish moving the user names to the box on the right.

   A confirmation page appears.

7. Click the **Continue** button.

   The Users & Groups: View Code Deployment Group page appears. You can continue modifying Code Deployment Groups, or you can select another function.

Chapter 4: Server Management Configuration

IN THIS CHAPTER

This chapter discusses the following topics:

- Ways to Configure Server Management
- Customer Accounts in Opsware SAS
- Customer Account Administration
- Server Attributes
- IP Range Groups and IP Ranges

Ways to Configure Server Management

Opsware SAS includes several ways to control the ways that servers are managed in your operational environment:

- Creating customers in Opsware SAS and associating servers in the operational environment with those customers.
- Setting up IP range groups and IP ranges so that servers are automatically associated with customers when Opsware users install the Opsware Agent on servers running in the operational environment
- Creating and modifying the values for Server Attributes so that Opsware users can identify broad categories of servers and what they are used for, as well as to describe their various stages of life cycle deployment.

Supported Operating Systems for Managed Servers

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

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

For the supported operating systems for Opsware Agents, Opsware 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 4-1: Opsware Agent Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR OPSWARE 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
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

Table 4-1: Opsware Agent Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS
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 4-2: OCC Client Supported Operating Systems

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

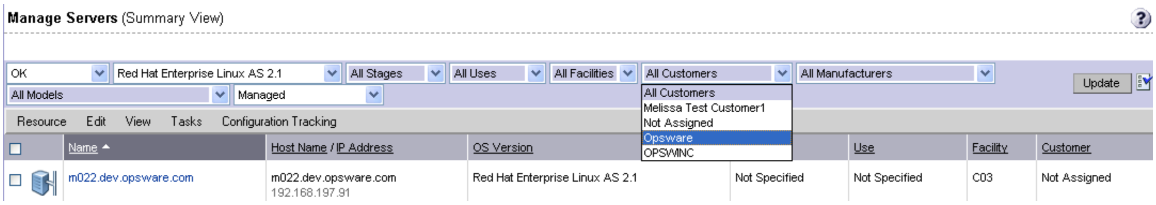
Customer Accounts in Opsware SAS

Many enterprise customers have consolidated disparate IT operations into a single operation, yet they still need separate reporting, billing, and management for different business units or groups (for example, West Coast Office, East Coast Office, and London Office).

Opsware SAS accommodates these requirements. Within the Opsware Command Center, Opsware users perform server provisioning and management by using customer accounts.

When an Opsware administrator creates a customer in Opsware SAS, a value for that customer is automatically added to the customer filter in the Managed Servers list, as Figure 4-1 shows.

Figure 4-1: Customer Filter in the Managed Servers List



Manage Servers (Summary View)

OK | Red Hat Enterprise Linux AS 2.1 | All Stages | All Uses | All Facilities | All Customers | All Manufacturers

All Models | Managed

□	Name ▲	Host Name / IP Address	OS Version		Use	Facility	Customer
□	m022.dev.opsware.com	m022.dev.opsware.com 192.168.197.91	Red Hat Enterprise Linux AS 2.1	Not Specified	Not Specified	C03	Not Assigned

By using customer accounts in the Opsware Command Center, you can segregate servers that belong to different business units. By segregating servers, you can have separate accounting for each customer or different levels of security for different customers. You might want to segregate the servers based on the department or business unit to which they belong for many reasons.

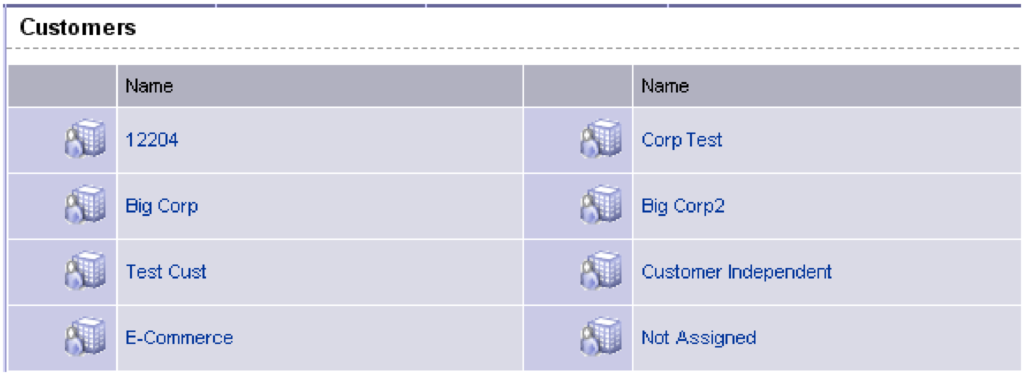
By default, Opsware SAS is shipped with the following two customers:

- Customer Independent – A global customer in Opsware SAS. Resources (applications, patches, and templates) that are associated with “Customer Independent” can be installed on any managed server, no matter what customer it is associated with.
- Not assigned – The servers are not associated with a customer. You can install applications, patches, or templates that are *Customer Independent* on *Not Assigned* servers. However, you cannot install or use any resources associated with a customer on a server that is not assigned to a customer.

When you assimilate a server into Opsware SAS, the server is associated with the *Not Assigned* customer if IP ranges were not created to automatically associate assimilated servers with customers. See Figure 4-2.

Opsware Inc. recommends that you associate servers with customers, if necessary, by using the Server Properties pages. See the *Opsware® SAS 5.2 User's Guide* for more information on editing the properties of a server.

Figure 4-2: Customers List Under Environment in the Opsware Command Center



Customers

	Name		Name
	12204		Corp Test
	Big Corp		Big Corp2
	Test Cust		Customer Independent
	E-Commerce		Not Assigned

Associated Servers with Customers

An Opsware user or an Opsware administrator can set up an IP range group so that servers are automatically associated with customers when users perform these server management tasks:

- Manage servers running in the operational environment by installing an Opsware Agent on the servers

  See the *Opsware® SAS 5.2 User's Guide* for more information on how to install an Opsware Agent.

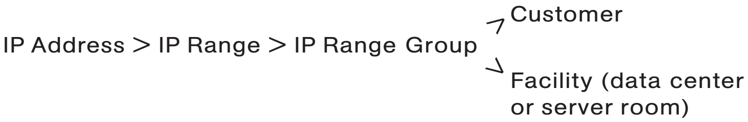
- Use the OS Provisioning feature to install operating systems on bare-metal servers

  See the *Opsware® SAS 5.2 User's Guide* for more information on OS provisioning.

To set up this automatic customer association, you must create IP range groups for customers and specify the ranges of IP addresses that the groups contain.

In the Opsware Command Center, an IP range group is both a physical and logical list – an accounting way to group ranges of IP address and assign them to a particular customer. An IP range identifies a range of IP addresses within an IP range group.

When you set this up, IP addresses get their customer association through the IP range, which, in turn, gets its customer association from the IP range group.



IP Address > IP Range > IP Range Group

Customer

Facility (data center or server room)

See “IP Range Groups and IP Ranges” on page 83 in this chapter for more information.

The loose relationship between server and IP address means that you can associate a server with a different customer from its IP address.

Even when IP range groups are set up for a customer, a server's IP address does not necessarily determine the customer to which the server is associated because a user can change the customer association in the Server Properties page.

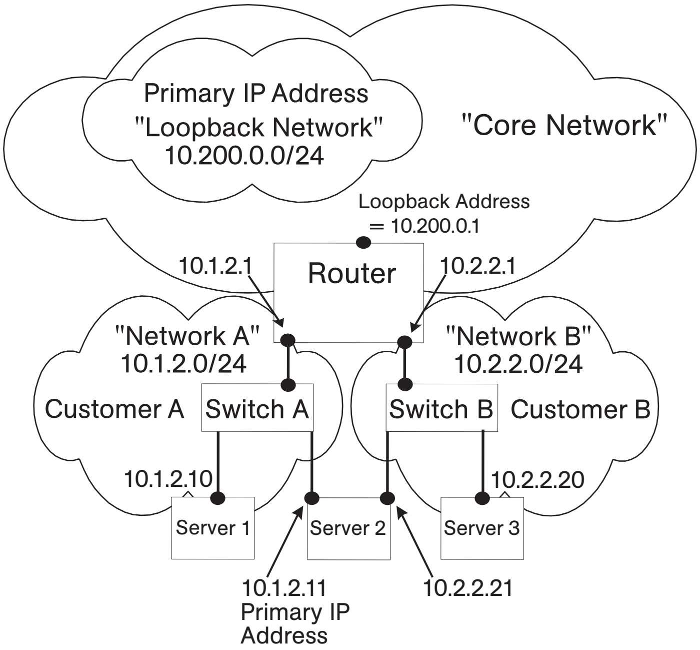
See *Opsware® SAS 5.2 User’s Guide* for information about how to change the customer association for a server.

The customer association for a server is based on the management IP address of the server and not the primary IP address.

See the *Opsware® SAS 5.2 User’s Guide* for more information about how Opsware SAS uses management IP addresses for servers.

However, a server always belongs to the same facility (data center or server room) as its primary IP address. Opsware SAS enforces the relationship between server and facility at hardware registration. See Figure 4-3.

Figure 4-3: Primary IP Addresses in Opsware SAS



In this illustration, the following conditions apply:

- Server 1 belongs to Customer A.
- Server 2 belongs to Customer A but has IP addresses in Network A and Network B.
- Server 3 belongs to Customer B.
- The Router belongs to the Core Network but has IP addresses in Network A and Network B.

Customer Account Administration

This section provides information about customer account administration within Opsware SAS and contains the following topics:

- Customer Account Administration Overview
- Creating a Customer
- Updating Customer Information and Settings
- Setting Custom Attributes for Customers
- Restrictions for Deleting Customers
- Deleting a Customer

Customer Account Administration Overview

As an Opsware administrator, you can add customers or update information and configuration settings for an existing customer.

Creating a Customer

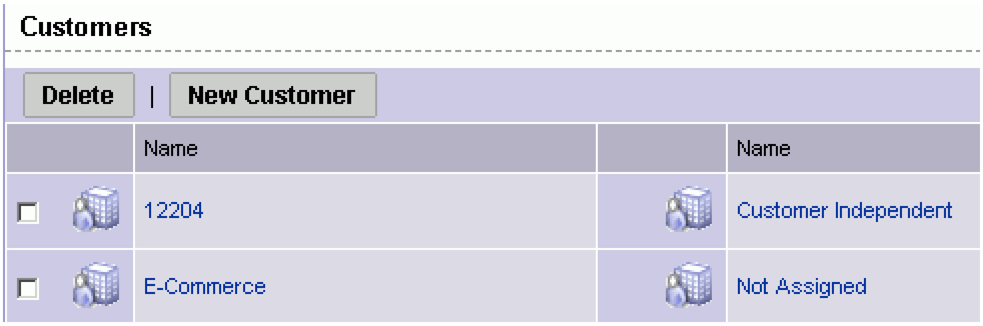
As an Opsware administrator, you can add customers to your Opsware SAS installation to create designations by business unit to provide management of Opsware SAS operations and configuration.

Perform the following steps to create a customer:

1 From the navigation panel, click Environment ➤ Customers.

The Customers page displays a list of all current customers, as Figure 4-4 shows.

Figure 4-4: List of Current Customers on Customers Page

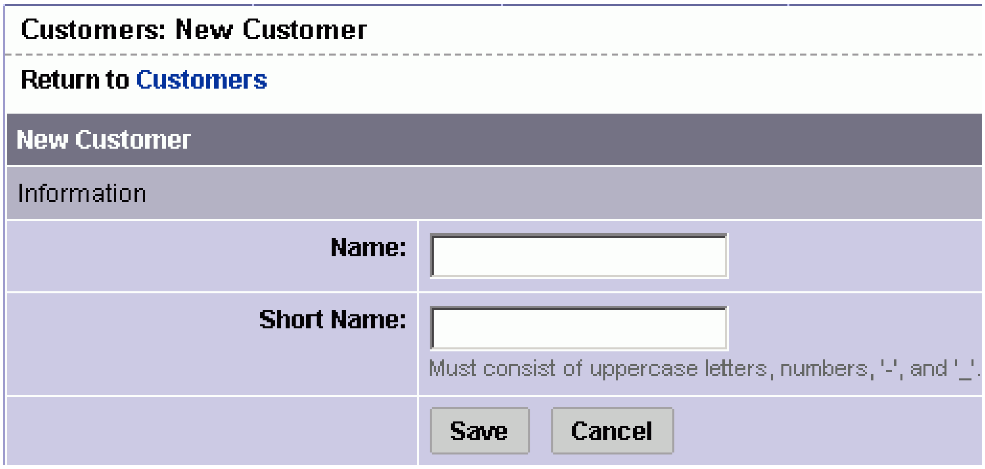


		Name		Name
□		12204		Customer Independent
□		E-Commerce		Not Assigned

2 Click the New Customer button.

The Customer: New Customer page appears where you can define the settings for a customer account, as Figure 4-5 shows.

Figure 4-5: Information Section of New Customer Page



Customers: New Customer

Return to Customers

New Customer

Information

Name:

Short Name:

Must consist of uppercase letters, numbers, '-', and '_'.

3 In the Information section, enter a Name for the customer and a Short Name, or a nickname by which the customer name will display.

The short name is limited to 25 characters and must consist of uppercase letters, numbers, hyphens (-), and underscores (_).

4 If you have more than one facility, specify the associated facilities for the customer. To add a facility to the customer, select a facility from those displayed in the Available Facility list and click the left arrow button.

You only see the fields to add a facility for a customer when Opsware SAS is running in multiple facilities. See the *Opsware® SAS 5.2 Administration Guide* for more information about Opsware technology in multiple facilities.

5 When you finish defining the customer, click the Save button. A confirmation message appears that says that the customer was successfully created.

By default, no access permission of this customer is granted to any user groups. In order to permit users to access this customer, you must grant access permissions to the appropriate user groups.

6 Click the Continue button. The Manage Customer page appears.

You must log out and log in again to see the updated Customer list.

After you create a customer, you can define custom attributes for the customer. These custom attributes include setting miscellaneous parameters and named data values. Users can write scripts that use these parameters and data values when they perform a variety of functions, including network and server configuration, notifications, and CRON script configuration.

See “Setting Custom Attributes for Customers” on page 74 in this chapter for more information

Updating Customer Information and Settings

As an Opsware administrator, you can update information or change configuration settings for existing customer accounts defined for your Opsware SAS.

Perform the following steps to update an existing customer:

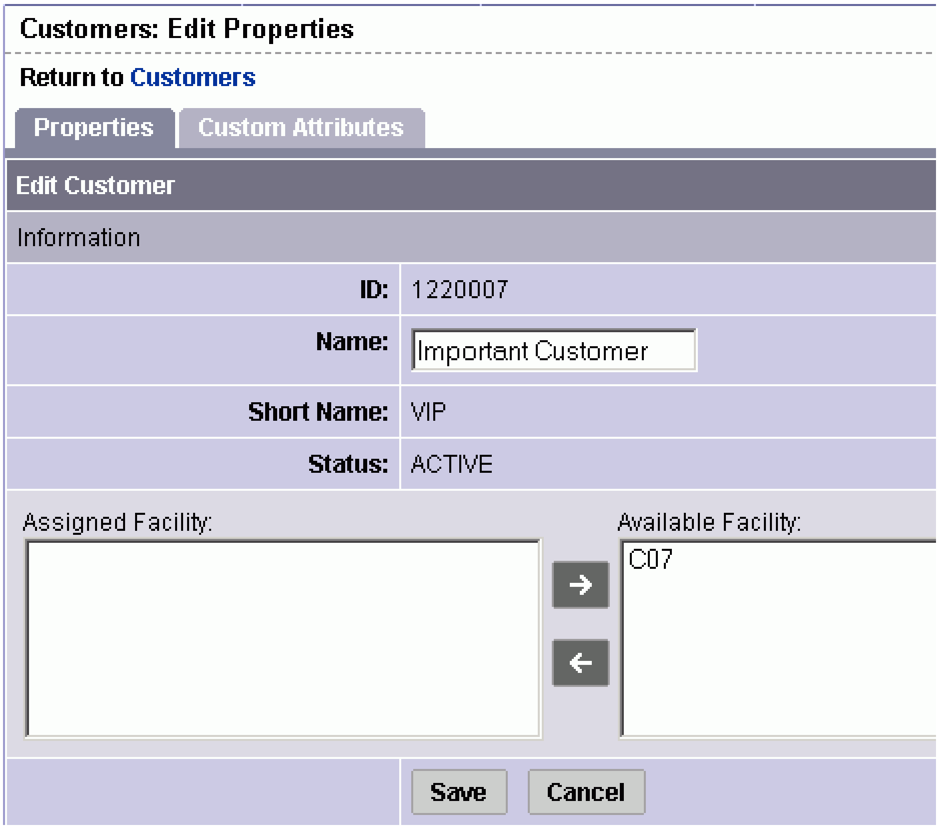
1 From the navigation panel, click Environment ➤ Customers. The Customers page appears, which shows a list of your existing customer accounts.

2 Click the hyperlinked name of the customer whom you want to update.

The Customers: Edit Properties page appears, as Figure 4-6 shows. The list box on the left side includes facilities assigned to the customer. The list box on the right side includes all other Opsware SAS-managed facilities that are available to be added for a new or existing customer.

To change the name for the customer who appears in the Opsware Command Center, edit the name that appears in the Name field.

Figure 4-6: Assign Facility Section of the Customers: Edit Properties Page



Customers: Edit Properties

Return to Customers

ID: 1220007

Name: Important Customer

Short Name: VIP

Status: ACTIVE

Assigned Facility:

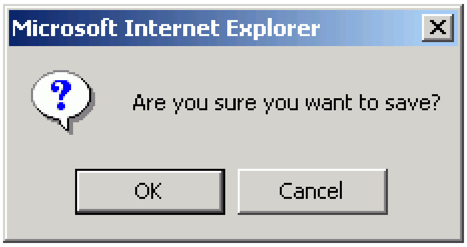
Available Facility: C07

3. To add a facility to the customer, select a facility from those displayed in the Available Facility list and click the left arrow button.

4. Click the Save button.

A message appears that confirms that you want to save the changes you just made, as Figure 4-7 shows.

Figure 4-7: Confirm Save Message



Microsoft Internet Explorer

Are you sure you want to save?

5 Click the OK button to save the changes.

The Customers page appears, which allows you to continue making changes to customer properties.

Setting Custom Attributes for Customers

You can use the Custom Attribute function to apply special properties to customers.

Perform the following steps to apply special properties to customers:

1 From the navigation panel, click Environment ➤ Customers. The Customers page appears, which shows a list of your existing customer accounts.

2 Click the hyperlinked name of the customer who you want to update.

The Customers: Edit Properties page appears.

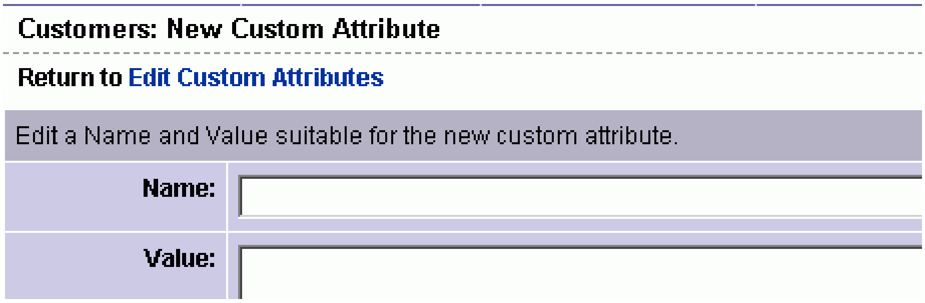
3 Click the Custom Attributes tab.

The Customers: Edit Custom Attributes page appears. If custom attributes have previously been applied to this customer, they appear on this page.

4 Click the New button.

The Opsware Command Center displays the Customers: New Custom Attributes page, as Figure 4-8 shows.

Figure 4-8: New Custom Attributes Page



Customers: New Custom Attribute

Return to Edit Custom Attributes

Edit a Name and Value suitable for the new custom attribute.

These named values are used to provide parameters to Opsware SAS, for example, to customize displays or provide settings to use during installation or configuration of packaged software in the operational environment.

Do not use either an asterisk (*) or a question mark (?) in the name field.

Be careful when you update or remove existing attribute settings as it might affect or disrupt operation of the operational environment. Contact your Opsware, Inc. Support Representative to help you determine the appropriate changes to make when you update the information or settings for a specific customer.

5 When you finish entering names and values, click the Save button, or exit without entering any values by clicking the Return to Customers link.

Restrictions for Deleting Customers

You can only delete a customer account from the Opsware Command Center when the following conditions are true for the customer:

- No Nodes are attached to the customer account.
- The customer account does not own any software packages; the packages uploaded for the customer must be deleted or deprecated.

- All servers assigned to the customer are deactivated.
- No IP Range Groups are created for the customer.
- No IP Ranges are created for the customer.
- No server groups are created for the customer.

If any of these restrictions apply to this customer, a message appears and you cannot delete the customer.

If the restrictions do not apply, the user is prompted to move deactivated servers to the Not Assigned customer account.

Deleting a Customer

Deleting a customer removes the customer information from Opsware SAS and moves deactivated servers assigned to the customer to the Not Assigned customer account or deletes the data about the servers from the Model Repository database.

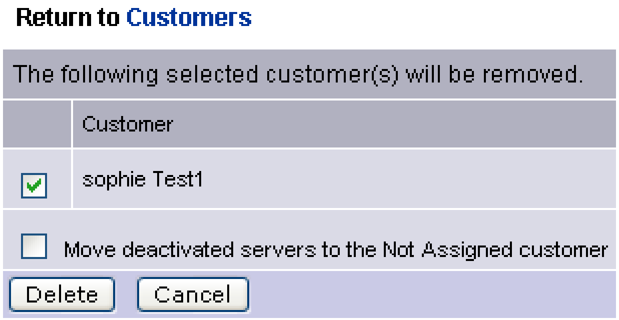
See "Restrictions for Deleting Customers" on page 75 in this chapter for more information

Perform the following steps to delete a customer:

1. From the navigation panel, click Environment ➤ Customers. The Customers page appears, which shows a list of your existing customer accounts.
2. Select the check box next to the customer whom you want to delete.
3. Click the Delete button.

   A confirmation page appears, which verifies that the selected customer will be deleted, as Figure 4-9 shows.

Figure 4-9: Customers: Delete Confirmation Page



Return to Customers

The following selected customer(s) will be removed.

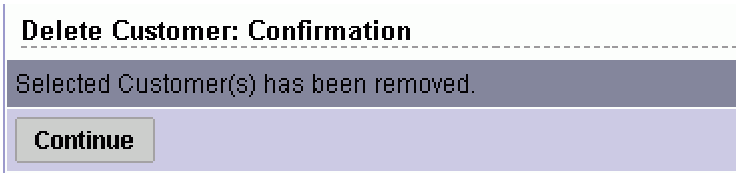
	Customer
☑	sophie Test1

☐ Move deactivated servers to the Not Assigned customer

4. Click the Delete button.

A confirmation page appears, as Figure 4-10 shows.

Figure 4-10: Delete Customer: Confirmation Page



Delete Customer: Confirmation

Selected Customer(s) has been removed.

5 Click the Continue button.

The Opsware Command Center displays the updated Customers page.

Server Attributes

This section provides information about server attributes within Opsware SAS and contains the following topics:

- Server Attributes Overview
- Creating Server Use Values
- Editing Server Use Values
- Deleting Server Use Categories
- Creating Deployment Stage Values
- Editing Deployment Stage Values
- Deleting Deployment Stage Values

Server Attributes Overview

The Server Attribute function is used to identify broad categories of servers and what they are used for, as well as to describe their various stages of life cycle deployment.

Opsware SAS comes with three Server Use categories already defined (and which cannot be changed or deleted): Not Specified, Production, and Staging. It also has a Deployment Stage category pre-defined - Not Specified - (which also cannot be changed or deleted).

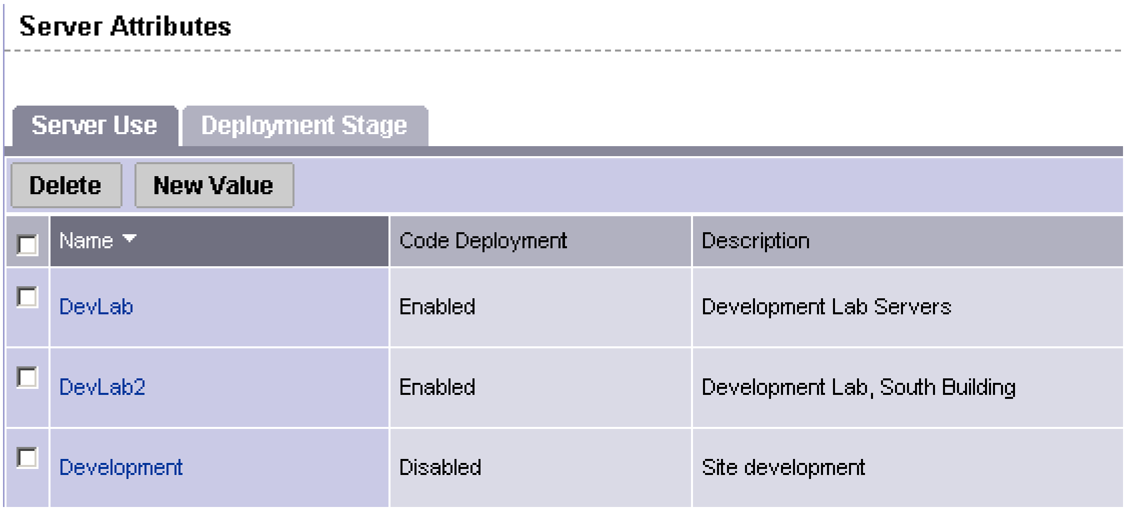
The attributes defined here, along with the default attributes, populate two lists in the Server Management function: Server Use and Deployment Stage. See the *Opsware*® *SAS 5.2 User's Guide* for more information.

Creating Server Use Values

Perform the following steps to create server use values:

1. From the navigation panel, select Administration ➤ Server Attributes. The Server Attributes page appears with the Server Use tab displayed, which shows all previously defined server use categories, as Figure 4-11 shows.

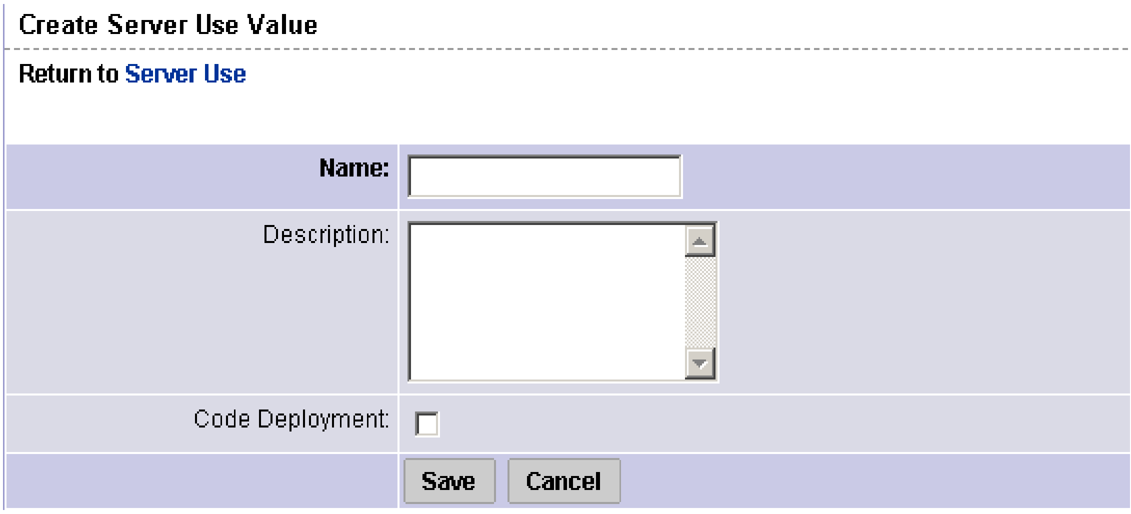
Figure 4-11: Server Use Tab of the Server Attributes Function



□	Name ▼	Code Deployment	Description
□	DevLab	Enabled	Development Lab Servers
□	DevLab2	Enabled	Development Lab, South Building
□	Development	Disabled	Site development

2. Click the New Value button. The Create Server Use Value page appears, as Figure 4-12 shows.

Figure 4-12: Create Server Use Value Page



Name:	
Description:	
Code Deployment:	□

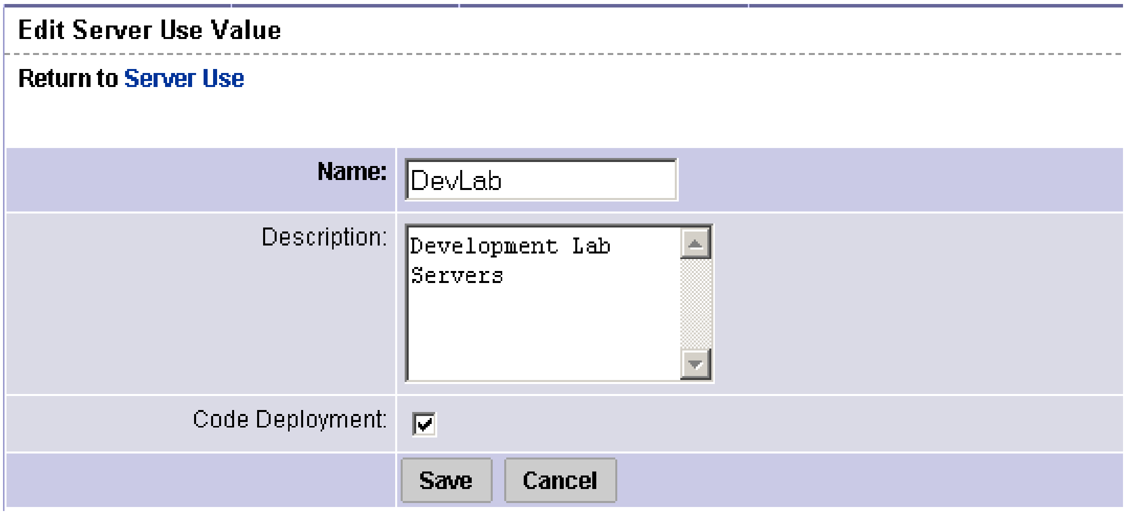
3. Enter the name of the Server Use category that you want to create. This name appears in the Server Use list in the Managed Servers area of the system. This field is required.
4. Enter a description of the server use value that you are defining.
5. Click the Code Deployment check box if you want this server use category to also appear in the Code Deployment list.
6. Click the Save button.

Editing Server Use Values

Perform the following steps to edit server use values:

1. From the navigation panel, select Administration ➤ Server Attributes. The Server Attributes page appears with the Server Use tab displayed, which shows all previously-defined server use categories.
2. The names of the server use categories that you already defined, as well as the default categories names, are hyperlinks. Click the link to edit the values of the categories. The Edit Server Use Value page appears, as Figure 4-13 shows.

Figure 4-13: Edit Server Use Value Page



Edit Server Use Value

Return to Server Use

Name:	DevLab
Description:	Development Lab Servers
Code Deployment:	☑

For the default categories of Not Specified, Production, and Staging, only the description can be modified.

For the server use categories that you have defined, all values can be modified.

3. Make any necessary changes to the Name, Description, or Code Deployment fields.
4. Click the Save button.

Deleting Server Use Categories

Perform the following steps to delete the server use categories:

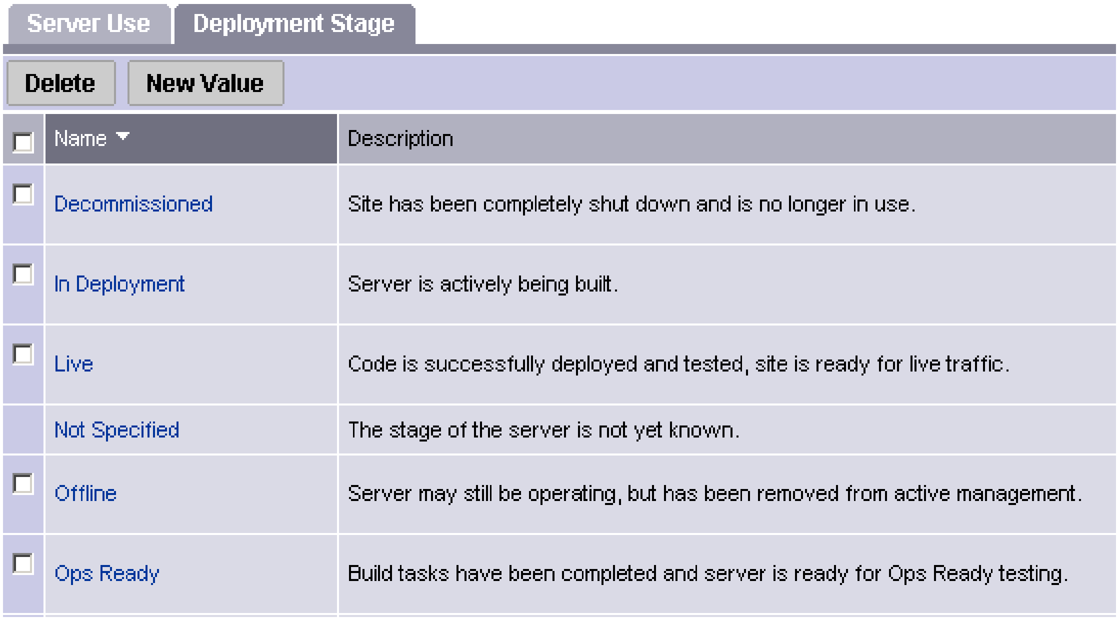
1. From the navigation panel, select Administration ➤ Server Attributes. The Server Attributes page appears with the Server Use tab displayed, which shows all previously-defined server use categories.
2. Click the check box next to each of the server use categories that you want to delete. You cannot delete the ones with no check boxes - Not Specified, Production, and Staging.
3. Click the Delete button. A confirmation window appears. You can view or hide the details of the server uses that you are about to delete.
4. Click the Delete button. The server use values are deleted, and the Server Attributes page refreshes, which shows the remaining serve use values.

Creating Deployment Stage Values

Perform the following steps to create deployment stage values:

1. From the navigation panel, select Administration ➤ Server Attributes. The Server Attributes page appears with the Server Use tab displayed, which shows all previously-defined server use categories.
2. Click the Deployment Stage tab. The list of previously defined deployment stages appears, as Figure 4-14 shows.

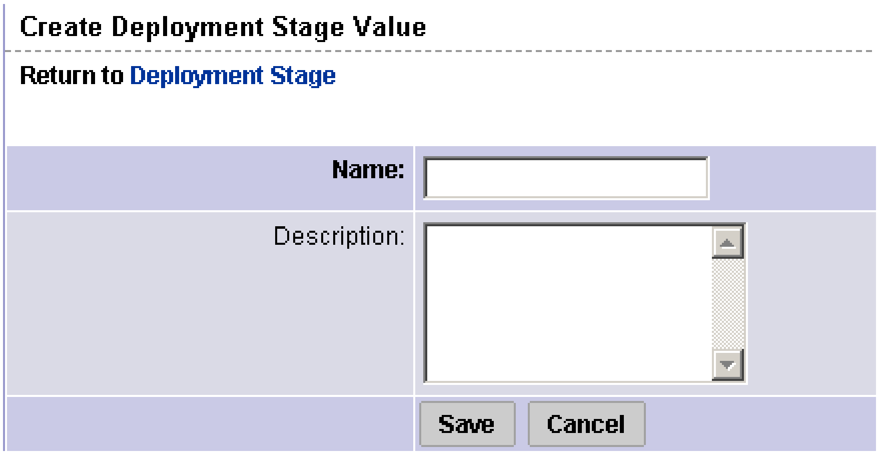
Figure 4-14: Deployment Stage Tab of the Server Attributes Function



□	Name ▾	Description
□	Decommissioned	Site has been completely shut down and is no longer in use.
□	In Deployment	Server is actively being built.
□	Live	Code is successfully deployed and tested, site is ready for live traffic.
	Not Specified	The stage of the server is not yet known.
□	Offline	Server may still be operating, but has been removed from active management.
□	Ops Ready	Build tasks have been completed and server is ready for Ops Ready testing.

3 Click the New Value button. The Create Deployment Stage Value page appears, as Figure 4-15 shows.

Figure 4-15: Create Deployment Stage Value Page



Create Deployment Stage Value

Return to Deployment Stage

Name:	
Description:	

4 Enter the Name of the deployment stage. This field is required.

5 Enter a description of the deployment stage.

6 Click the Save button.

Editing Deployment Stage Values

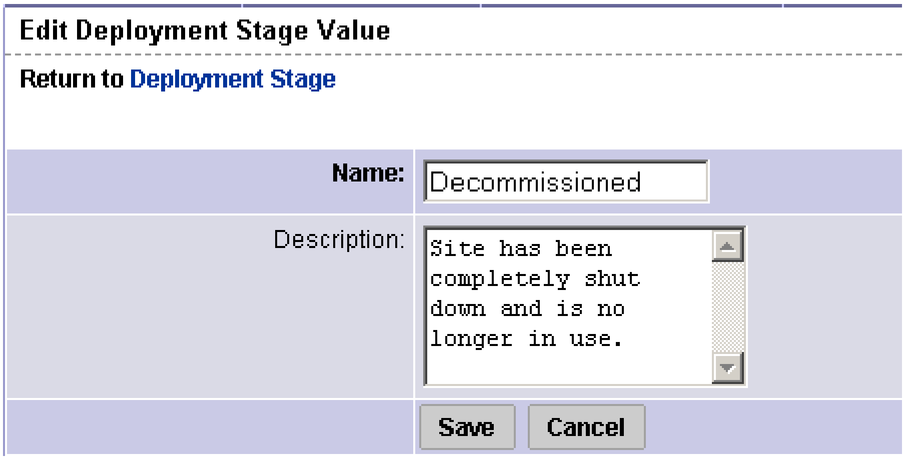
Perform the following steps to edit deployment stage values:

1 From the navigation panel, select Administration ➤ Server Attributes. The Server Attributes page appears with the Server Use tab displayed, which shows all previously defined server use categories.

2 Click the Deployment Stage tab. The list of previously defined deployment stages appears.

3 Each of the deployment stages on the list is a hyperlink. Click the name of the deployment stage whose values you want to edit. The Edit Deployment Stage Value page appears, as Figure 4-16 shows.

Figure 4-16: Edit Deployment Stage Value Page



Edit Deployment Stage Value

Return to Deployment Stage

Name: Decommissioned

Description: Site has been completely shut down and is no longer in use.

4 Change the Name or Description as necessary.

5 Click the Save button.

Deleting Deployment Stage Values

Perform the following steps to delete deployment stage values:

1 From the navigation panel, select Administration ➤ Server Attributes. The Server Attributes page appears with the Server Use tab displayed.

2 Click the Deployment Stage tab. The list of previously defined deployment stages appears.

3 Click the check box next to the deployment stage that you want to delete. The one with no check box, Not Specified, cannot be deleted.

4 Click the Delete button. A confirmation page appears. You can view or hide the details of the deployment stages that you are about to delete.

5 Click Delete. The Server Attributes page with the Deployment Stage tab appears, which shows the remaining deployment stages.

IP Range Groups and IP Ranges

This section provides information on IP range groups and IP ranges within Opsware SAS and contains the following topics:

- IP Range Groups and IP Ranges Overview
- Creating an IP Range Group
- Creating an IP Range
- Changing Address Ranges on IP Ranges
- Increasing and Decreasing the Prefix Length
- Changing the Status of an IP Address in an IP Range

IP Range Groups and IP Ranges Overview

An Opsware user or an Opsware administrator can set up IP range groups and IP ranges so that servers are automatically associated with customers when users perform the following server management tasks:

- Manage servers running the operational environment by installing an Opsware Agent on the servers

  See the *Opsware® SAS 5.2 User's Guide* for more information on installing an Opsware Agent on a server.

- Use the OS Provisioning feature to install operating systems on bare-metal servers

If you do not assign an IP range group to a customer, by default, a server is not assigned to a customer (Not Assigned appears in the Customer column of the server list) when you install an Opsware Agent on the server.

An IP Range Group is a group of IP ranges that belong to a customer. It is both a physical and logical list – an accounting way to group IP ranges and assign them to a specific customer.

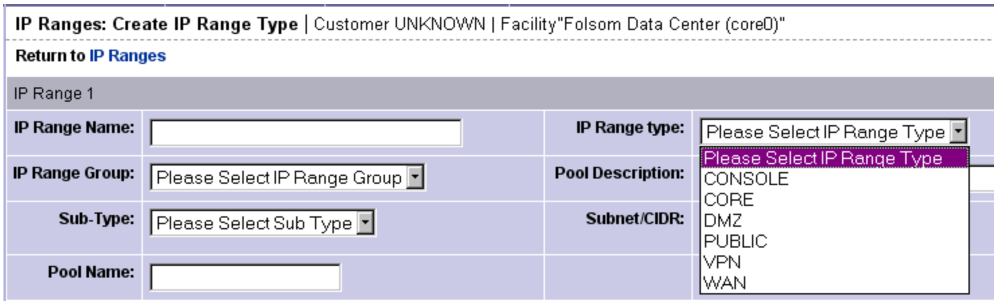
In the Opsware Command Center, an IP range identifies a range of IP addresses (in the OSI model – layer 3 IP address ranges). Each IP range can contain many IP addresses. The range of IP addresses is dependent on the subnet specified.

There is no direct association of an IP range with a specific customer; an IP range inherits its association to a customer from the IP Range Group it is created in.

See See "Customer Account Administration" on page 70 in Chapter 4 for more information for more information about Associated Servers with Customers.

Several types of IP Ranges are available in the Opsware Command Center, as Figure 4-17 shows.

Figure 4-17: Types of IP Ranges in the Opsware Command Center



IP Ranges: Create IP Range Type | Customer UNKNOWN | Facility"Folsom Data Center (core0)"

Return to IP Ranges

IP Range 1

IP Range Name:

IP Range Group: Please Select IP Range Group

Sub-Type: Please Select Sub Type

Pool Name:

IP Range type: Please Select IP Range Type

Pool Description:

Subnet/CIDR:

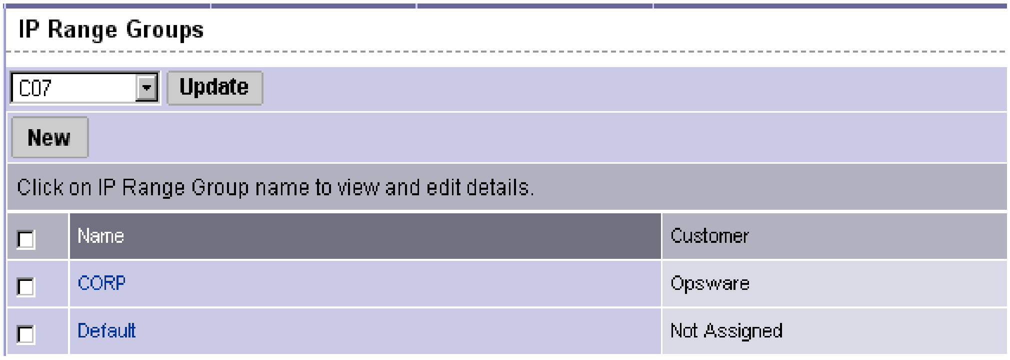
Creating an IP Range Group

You perform this task to create a group of IP ranges for a specific customer. After you create the group, you can designate the IP ranges that you want in that group.

Perform the following steps to create an IP Range Group:

1. From the navigation panel, click Environment ➤ IP Range Groups. The IP Range Groups page appears, as Figure 4-18 shows.

Figure 4-18: IP Range Groups Page in the Opsware Command Center



IP Range Groups

C07 ▾ Update

New

Click on IP Range Group name to view and edit details.

□	Name	Customer
□	CORP	Opsware
□	Default	Not Assigned

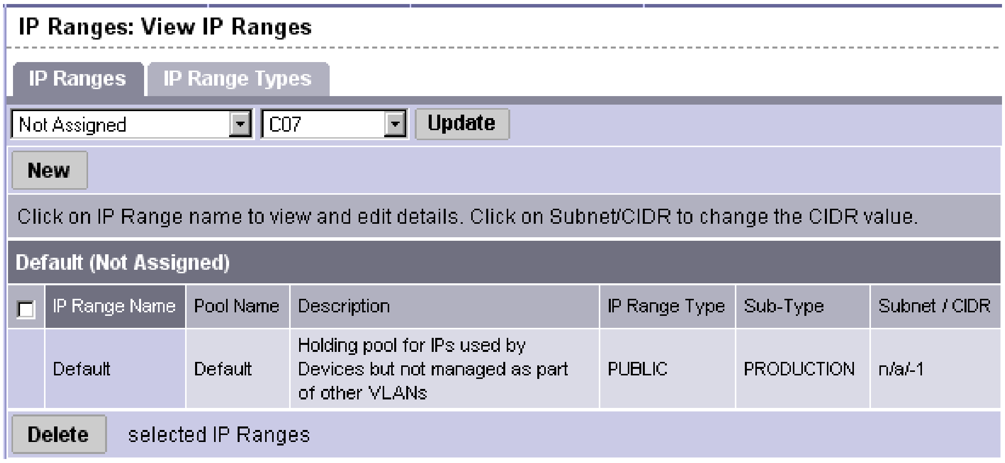
2. From the list, select the facility in which you want to create the IP range group and click the Update button. The list of IP range groups for that facility appears.
3. Click the New button at the top of the page. The IP Range Groups: Create IP Range Group page appears.
4. Enter a name for the new IP range group.
5. Select the customer from the drop-down list.
6. Click the Save button.

Creating an IP Range

Perform the following steps to create an IP Range:

1 From the navigation panel, click Environment ➤ IP Ranges. The IP Ranges: View IP Ranges page appears, as Figure 4-19 shows.

Figure 4-19: IP Ranges for the Default Customer ("Not Assigned")



IP Ranges: View IP Ranges

Click on IP Range name to view and edit details. Click on Subnet/CIDR to change the CIDR value.

Default (Not Assigned)

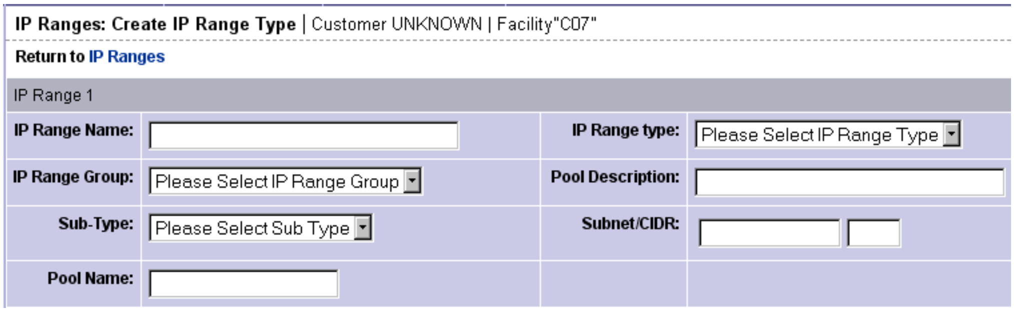
□	IP Range Name	Pool Name	Description	IP Range Type	Sub-Type	Subnet / CIDR
	Default	Default	Holding pool for IPs used by Devices but not managed as part of other VLANs	PUBLIC	PRODUCTION	n/a/-1

Delete selected IP Ranges

2 From the list, select the customer and facility in which you want to create the IP range and click the Update button. The list of IP ranges for that customer and facility appears.

3 Click the New button at the top of the page. The IP Ranges: Create IP Range Type page appears, as Figure 4-20 shows. You can add up to five new IP ranges at a time.

Figure 4-20: Creating an IP Range



IP Ranges: Create IP Range Type | Customer UNKNOWN | Facility"C07"

Return to IP Ranges

IP Range 1

IP Range Name:		IP Range type:	Please Select IP Range Type
IP Range Group:	Please Select IP Range Group	Pool Description:	
Sub-Type:	Please Select Sub Type	Subnet/CIDR:	
Pool Name:			

4 Define the following properties for each IP range:

- IP Range Name (for example, VLAN999 or SERVER100)
- IP Range Group – a customer might have several IP range groups and you must select one for the IP range that you are creating
- Sub-Type (for example, Development, Production, Staging, and so forth)

- Pool Name (for example, SAMPLE CUSTOMER SERVER pool)
- IP Range Type (for example, SERVER, PUBLIC, CONSOLE, TRANSIT, CORE, and so forth)
- Pool Description – provides detailed information about the IP range
- Subnet (for example, 10.2.0.0)
- Mask or Prefix Length – enter the prefix length or netmask (for example, 24, for /24, a netmask 255.255.255.0) in the CIDR field

You must complete all fields for each new IP range, which assumes that you have specific knowledge of your network's configuration and know the correct entries to include.

5. After you complete all entries, click the Save button at the bottom of the page.

Changing Address Ranges on IP Ranges

Classless Inter-Domain Routing (CIDR) in Opsware SAS provides a way of specifying a range of IP addresses to include in an IP range.

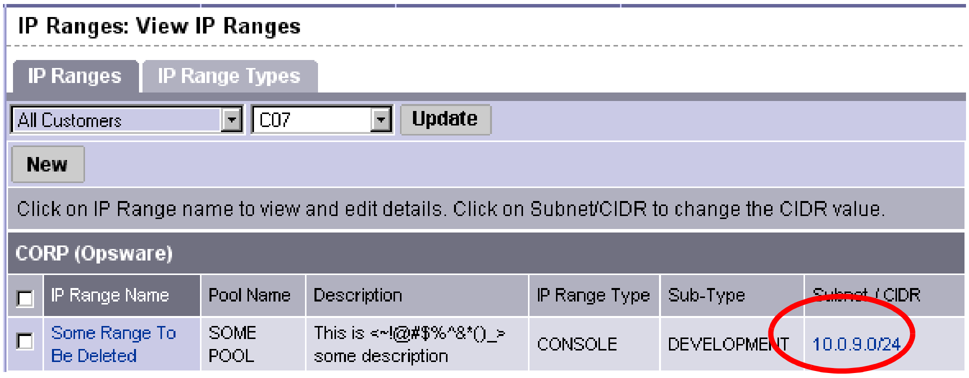
Opsware SAS might take several minutes to display an IP range with many IP addresses. For example, an IP Range with CIDR 19 (which has 8,192 IP addresses) might take 5 minutes to display in the Opsware Command Center.

Perform the following steps to change address ranges on IP ranges:

1. From the navigation panel, click Environment ➤ IP Ranges. The IP Ranges: View IP Ranges page appears.
2. From the list, select the customer and facility whose IP range you want to update and click the Update button. The list of IP ranges for that customer and facility appears.

3. Click the SUBNET/CIDR link at the end of the row for the IP range that you want to change, as Figure 4-21 shows.

Figure 4-21: IP Ranges in the Opsware Command Center



Click on IP Range name to view and edit details. Click on Subnet/CIDR to change the CIDR value.

CORP (Opsware)

□	IP Range Name	Pool Name	Description	IP Range Type	Sub-Type	Subnet / CIDR
□	Some Range To Be Deleted	SOME POOL	This is <~!@#$%^&*()_> some description	CONSOLE	DEVELOPMENT	10.0.9.0/24

The last two digits in the Subnet/CIDR column make up the current prefix length for a particular IP range. The IP Range: Change CIDR page appears.

4. To change the current CIDR setting, select a new value from the list in the New CIDR column.

5. Click the Change button.

Changing the prefix length in the Opsware Command Center does not automatically change the net masks of servers for the servers themselves.

Increasing and Decreasing the Prefix Length

You can use the Opsware Command Center to increase or decrease the length of an IP range.

Increasing the Prefix Length

Increasing the prefix length reduces the IP range size. For example, if you have an IP range with prefix length 24 and it has 256 IP addresses in it, changing the prefix length to 25 results in the creation of two IP ranges with prefix length 25, each containing 128 IP addresses.

Example:

```
Network A – 10.1.0.0/24
```

Becomes:

```
Network A – 10.1.0.0/25
Network B: 10.1.0.128/25 (new network)
```

Decreasing the Prefix Length

Decreasing the prefix length expands the IP range size. Take the two CIDR 25 IP ranges from above. On the first IP range, changing the prefix length to 24 results in one IP range that contains twice as many IP addresses as before. The two original CIDR 25 IP ranges are combined to make one larger CIDR 24 IP range.

Example:

```
Network A – 10.1.0.0/24
```

```
Network B – 10.1.1.0/24
```

Becomes:

```
Network AB: 10.1.0.0/23 (one network)
```

This change only works if the two CIDR 25 IP ranges occupy contiguous blocks in the same IP range group. If they do not occupy contiguous blocks, you get an error message.

Changing the Status of an IP Address in an IP Range

You can use the IP Range feature to change the status of that IP address in the Opsware Command Center. For example, you might want to reserve an available IP address because you will assign it to a specific server in the next few days.

The status of an IP address automatically changes from available to assigned when a server with that IP address registers its hardware with Opsware SAS.

Perform the following steps to change the status of an IP address in an IP range:

1. From the navigation panel, click Environment ➤ IP Ranges. The IP Ranges: View IP Ranges page appears.

2. From the list, select the customer and facility for which you want to assign IP addresses and click the Update button. The list of IP ranges for that customer and facility appears.

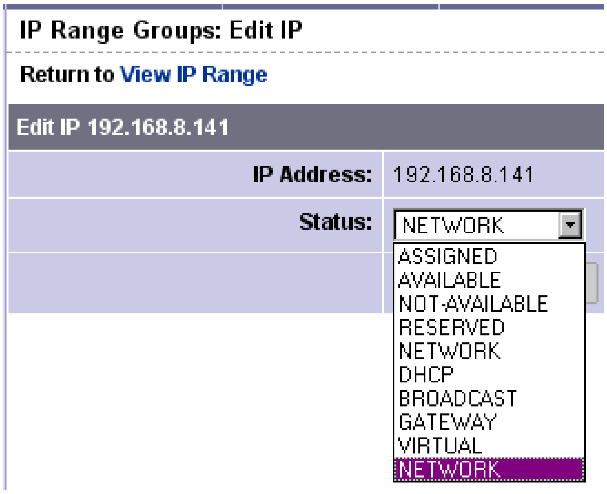
3. Click the name for the IP range in which you want to assign IP addresses. The IP Range: View IP Range page appears. By default, the View tab displays.

   The bottom of the page contains the IP addresses within that range. For each assigned or reserved IP address in the range, you can see its status.

4 Click an individual IP address link.

From the page that appears, you can change the status of the IP address (to ASSIGNED, AVAILABLE, RESERVED, and so forth). See Figure 4-22.

Figure 4-22: Editing the Properties of an IP Address in an IP Range



IP Range Groups: Edit IP

Return to View IP Range

Edit IP 192.168.8.141

IP Address: 192.168.8.141

Status: NETWORK

5 Select the status from the list. IP addresses can have one of the following statuses:

- ASSIGNED: A server is registered with this IP address.
- AVAILABLE: Available IP address.
- NOT AVAILABLE: Used to *reserve* an IP address for future use. For example, you might want to build a new server but need an IP address for the server prior to it being plugged into the network. Setting the status of an IP address to NOT AVAILABLE reserves it, so that another user does not take that IP address before the server is racked, stacked, and plugged into the network.
- RESERVED: The first couple of IP addresses after the first IP address is reserved
- NETWORK: Always assigned to the first IP address in a subnet
- DHCP: IP addresses reserved for use by a DHCP server
- BROADCAST: A special IP address reserved for sending a message to all stations
- GATEWAY: An IP address that acts as an entrance to another network
- VIRTUAL: Indicates a virtual IP address, such as

  www.samplecustomer.com

which is an IP address associated with a load balancer. The IP address does not correspond to any server, but yet the active load balancer responds to this request and forwards it to the appropriate Web server.

6. Click the Save button.

Chapter 5: OS Provisioning Setup

IN THIS CHAPTER

This chapter discusses the following topics:

- OS Provisioning Setup
- OS Media Management
- Additional Windows NT Media Setup Tasks
- Operating System Definitions
- Build Customization Scripts
- Working with OS Definitions
- Default Values for the OS Build Process
- Overview of Including OS Definitions in Templates
- Hardware Support in OS Provisioning

Before you set up the OS Provisioning feature, the OS provisioning components must have been installed in the local facility with the Opsware Installer and configured correctly. Contact your Opsware administrator for information about the installation and configuration of Opsware SAS OS provisioning components.

The OS Provisioning feature does not provision HP-UX or AIX operating systems out of the box; however, Opsware SAS can be integrated with Network Installation Management (NIM) to provision AIX and Ignite-UX to provision HP-UX. See "OS Installation Integration" on page 155 in Chapter 6 for more information. See the *Opsware® SAS 5.2 Deployment and Installation Guide* for information about how OS provisioning is configured during Opsware SAS installation.

OS Provisioning Setup

This section provides information on OS provisioning setup within Opsware SAS and contains the following topics:

- Overview of OS Provisioning Setup
- Process for Setting up OS Provisioning
- Setting Up for Sun Solaris OS Provisioning
- Setting Up for Linux OS Provisioning
- Setting Up for Microsoft Windows OS Provisioning

Overview of OS Provisioning Setup

Setting up the OS Provisioning feature is an ongoing process. Before you can provision servers with a new OS, you must set up the OS Provisioning feature to install that OS on the servers in your environment.

Additionally, you should continue to update existing operating systems with the latest patches and security fixes by updating the templates used to install the operating systems.

See "Overview of Including OS Definitions in Templates" on page 142 in this chapter for more information.

See "Patch Administration Using the Opsware Command Center" on page 343 in Chapter 11 for more information about how to set up patch management in Opsware SAS.

The OS Provisioning feature supports installation-based provisioning using Red Hat Linux Kickstart, SUSE Linux YaST2, Sun Solaris JumpStart, and Microsoft Windows unattended installation. Image-based provisioning requires customization that Opsware Professional Services can perform for your environment.

Contact your Opsware, Inc. Support Representative for information about using image-based provisioning with Opsware SAS.

Because the OS Provisioning feature supports installation-based provisioning, your organization can keep its OS installations very lean. Rather than trying to manage changing software through master images, you can use the OS Provisioning feature to install and remove often-changing software, including system patches, system utilities, and third-party agents (such as monitoring, backup, and anti-viral agents).

✓ You need a specific set of feature permissions to set up OS Provisioning. You'll also need permissions to access the OS definitions and templates. To obtain these permissions, contact your Opsware administrator. For more information, see "Permissions Reference" on page 409.

Process for Setting up OS Provisioning

An OS standards setter records in the OS Provisioning feature the standard configuration of an OS and its required utilities, drivers, and agents. System administrators can then use the OS Provisioning feature to install the OS, configure networking, and install other software required for smooth operation of the server.

Before you perform the tasks to set up OS provisioning, you must have a licensed copy of the OS installation media, which typically comes as a CD-ROM or DVD.

You must perform the following tasks to set up the OS Provisioning feature to install an OS:

1 Make the media for that OS available on the Media Server by performing these tasks:

1. Copy the OS media to the Media Server.
2. Create a Media Resource Locator (MRL) for the OS media by using the Opsware Import Media tool.

   See "OS Media Management" on page 101 in this chapter for more information.

2 Create a configuration file with a text editor to specify how the OS will be installed.

3 Prepare a definition in the Opsware Command Center for the OS by performing these tasks:

1. Indicate the location of the OS media by specifying the correct MRL.
2. Upload the configuration file into the OS Provisioning feature.

See “Defining an Operating System” on page 129 in this chapter for more information.

Setting Up for Sun Solaris OS Provisioning

The OS Provisioning feature includes a DHCP-based JumpStart configuration that hides the complexity of JumpStart from the end user. Unlike typical JumpStart systems, the OS Provisioning feature does not require configuration updates to the JumpStart server for each installation that you provision.

Instead, you prepare an OS definition in the OS Provisioning feature for each version of the Solaris OS that you want to install on servers in your environment.

The setup process for Solaris OS provisioning follows the general process for OS provisioning setup. However, you must perform certain setup tasks specifically for each Solaris OS. See the topics listed below.

1. Copying the Sun Solaris OS media to the Media Server by using the scripts included on the Sun Solaris installation CD-ROM or DVD.

   See “Prerequisites for Creating an MRL” on page 103 in this chapter for more information.

2. Creating an MRL for the Solaris media by using the Import Media tool.

   See “Creating an MRL with the Import Media Tool” on page 103 in this chapter for more information.

3. Creating a Solaris profile with a text editor.

   See “About Sun Solaris Profiles” on page 110 in this chapter for more information.

4. Preparing an OS definition for the Solaris OS in the Opsware Command Center by specifying the location of the Solaris OS media (with the MRL) and uploading the profile.

   See “Defining an Operating System” on page 129 in this chapter for more information.

5. Optionally, specifying a list of packages or clusters to install after the base OS installation is complete by adding the packages directly to the OS definition.

   See “About Conditional Packages for Solaris” on page 128 in this chapter for more information.

See "Overview of Installation Order for Solaris and Linux" on page 128 in this chapter for more information.

See "Modifying Which Packages an OS Definition Installs" on page 136 in this chapter for more information.

6 Customizing the default build process that the OS Provisioning feature uses to install the version of Solaris on servers.

See "About the Solaris Build Customization Script" on page 119 in this chapter for more information.

See "Requirements for Solaris Build Customization Scripts" on page 120 in this chapter for more information.

7 Editing the OS definition for the version of Solaris after you have created it so that it passes specific information to the Solaris build script to configure aspects of the installation process.

See "Default Values for the OS Build Process" on page 138 in this chapter for more information.

See "Custom Attributes for Sun Solaris" on page 139 in this chapter for more information.

Setting Up for Linux OS Provisioning

The OS Provisioning feature includes a Kickstart and YaST2 system that hides the complexity of Kickstart and YaST2 from the end user.

Unlike typical Kickstart or YaST2 systems, mapping a specific installation client to a particular configuration is a simple procedure in the OS Provisioning feature. In the OS Provisioning feature, each Linux OS (and template) has a single configuration associated with them.

The setup process for Linux OS provisioning follows the general process for OS provisioning setup. However, you must perform certain setup tasks specifically for the Linux OS. See the topics listed below.

1 Copying the Linux OS media to the Media Server.

See "Prerequisites for Creating an MRL" on page 103 in this chapter for more information.

2 Copying the Linux OS media to the Media Server.

See "Creating an MRL with the Import Media Tool" on page 103 in this chapter for more information.

3 Creating a configuration file with a text editor.

See "About Red Hat Linux Configuration Files" on page 111 in this chapter for more information.

See "About SUSE Linux Configuration Files" on page 111 in this chapter for more information.

4 Preparing an OS definition for the Linux OS in the Opsware Command Center by specifying the location of the Linux OS media (with the MRL) and uploading the configuration file.

See "Defining an Operating System" on page 129 in this chapter for more information.

5 Optionally, specifying a list of packages to install after the base OS installation is complete by adding the packages directly to the OS definition.

See "Overview of Installation Order for Solaris and Linux" on page 128 in this chapter for more information.

See "Modifying Which Packages an OS Definition Installs" on page 136 in this chapter for more information.

6 Customizing the default build process that the OS Provisioning feature uses to install the version of Linux on servers.

See "About Linux Build Customization Scripts" on page 124 in this chapter for more information.

See "Requirements for Linux Build Customization Scripts" on page 125 in this chapter for more information.

7 Editing the OS definition for the version of Linux after you have created it so that it passes specific information to the Linux build script to configure aspects of the installation process.

See "Default Values for the OS Build Process" on page 138 in this chapter for more information.

See "Custom Attributes for Linux" on page 140 in this chapter for more information.

8. Additionally, if necessary, adding new hardware support to a Linux build image. The OS Provisioning feature includes build images that install the target OS on servers for Linux.

   See “Adding Hardware Support to a Linux Build Image” on page 151 in this chapter for more information.

Setting Up for Microsoft Windows OS Provisioning

To prepare a Windows OS definition, you must set up a Windows unattended installation. You need to provide the following items when you set up Windows provisioning in Opsware SAS:

- A licensed copy of the Windows OS installation media, which typically comes as a CD-ROM or DVD
- Mass storage drivers and network interface card (NIC) drivers. The latest drivers can usually be downloaded from the hardware vendor's website.
- A Windows setup response file

The setup process for Windows OS provisioning follows the general process for OS provisioning setup. However, you must perform certain setup tasks specifically for the Windows OS. See the topics listed below.

1. Copying the Windows OS media to the Media Server.

   See “Prerequisites for Creating an MRL” on page 103 in this chapter for more information.

2. For the Windows NT media, modifying the media from the vendor to install Service Pack 6a and applying Microsoft patch Q143473 to the media.

   See “Additional Windows NT Media Setup Tasks” on page 106 in this chapter for more information.

3. Creating an MRL for the Windows media by using the Import Media tool.

   See “Creating an MRL with the Import Media Tool” on page 103 in this chapter for more information.

4. Creating a Windows response file with a text editor.

   See “About Microsoft Windows Response Files” on page 112 in this chapter for more information.

5 Preparing an OS definition for the Windows OS in the Opsware Command Center by specifying the location of the Windows OS media (with the MRL) and uploading the response file.

See “Defining an Operating System” on page 129 in this chapter for more information.

6 In the OS definition, uploading hardware-specific files for the hardware you expect to provision by mapping a signature for that hardware to the correct hardware-specific profile.

The OS Provisioning feature will select the correct Hardware Signature file at build time based on the hardware signature of the server that is about to be provisioned.

See “About Hardware Signature Files for Windows” on page 128 in this chapter for more information.

7 Optionally, specifying a list of packages to install after the base OS installation is complete by adding the packages directly to the OS definition.

See “Modifying Which Packages an OS Definition Installs” on page 136 in this chapter for more information.

8 Customizing the default build process that the OS Provisioning feature uses to install the version of Windows on servers.

See “About Windows Build Customization Scripts” on page 127 in this chapter for more information

9 Editing the OS definition for the version of Windows after you have created it so that it passes specific information to the Windows build script to configure aspects of the installation process

For a Windows OS definition, you can set a value for the timeout custom attribute. Setting this value controls the timeout value after an error.

See “Default Values for the OS Build Process” on page 138 in this chapter for more information.

See “Custom Attribute for Microsoft Windows” on page 141 in this chapter for more information.

10 If you need to boot x86-process based servers from a floppy (perhaps you cannot boot servers over the network), creating a Windows boot floppy

See “Creating a Windows Boot Image” on page 149 in this chapter for more information.

11 Additionally, if necessary, adding new hardware support to the Windows boot images

The default boot images for Windows include common NIC drivers for many hardware makes and models. Opsware SAS uses these NIC drivers to boot new x86-processor-based servers for the first time.

See “Adding NIC Support to a Windows Boot Image” on page 146 in this chapter for more information.

12 Updating the Windows PXE image after adding hardware support.

When Opsware SAS was installed with the Opsware Installer, an image was added to the PXE system by default. You only need to update the PXE image when you have added support for additional NIC drivers to the image.

See “Updating the PXE Image for Windows” on page 150 in this chapter for more information.

OS Media Management

This section provides information on OS media management within Opsware SAS and contains the following topics:

- Overview of OS Media Management
- Prerequisites for Creating an MRL
- Creating an MRL with the Import Media Tool
- Editing an MRL
- Deleting an MRL

Overview of OS Media Management

OS media consists of the installation software for an OS from the software vendor. Typically, OS media is distributed on CD-ROM, DVD, or by downloading the software distribution from the vendor’s FTP site. The OS media can contain binaries for installing the OS, packages of different types, metadata about the packages, and other information.

So that the OS Provisioning feature can access the media, you must copy it to the Opsware Media Server. The Media Server provides access to the OS media over the network by using NFS for Linux and Solaris OS provisioning, and by using SMB for Windows OS provisioning. After copying the OS media to the Media Server, you must import it into Opsware SAS by running the Opsware Import Media tool (a utility script included with Opsware SAS).

Running the Import Media tool creates an Opsware-generated string called a Media Resource Locator (MRL) for each OS media that you want to provision.

An MRL is a network path (in URI format) to the installation media for an OS on the Opsware Media Server. When a server is being provisioned with an OS, the server mounts the network path for the OS media by using NFS (for Linux and Solaris), or SMB (for Windows). The MRL is registered with Opsware SAS. An MRL should resolve to the Media Server in the local facility where Opsware SAS is installed.

To create an MRL, run the Media Import tool. Running the Import Media tool automatically performs the following functions:

- Mounts the media at the specified network path by using NFS or SMB
- Detects the OS (Solaris, Linux, or Windows) and version of the media
- Based on the server name and path that you specify, creates that MRL in Opsware SAS so that you can use it in OS definitions
- Extracts vendor-provided metadata (such as the package list and dependencies between packages) from the OS software and stores this data in Opsware SAS.
- For Sun Solaris and Linux, uploads all packages to the Software Repository so that the OS Provisioning feature can install them after initial OS provisioning

  For Solaris, an MRL represents or contains a path to the media for JumpStart purposes, a hierarchy of metaclusters, clusters, and packages, and information about package dependencies and installation order.

  For Linux, an MRL contains a path to the media for Kickstart or YaST2 and information about package dependencies and installation order.

  Re-running the Import Media tool with the same server and path as an existing MRL updates the MRL, but does *not* re-upload duplicate Linux or Solaris packages.
- For Linux and Microsoft Windows, modifies portions of the OS media to integrate the OS Provisioning feature with the vendor provisioning boot process.

Prerequisites for Creating an MRL

Before you run the Import Media tool, the OS media that you want to import must be available through the network on the Media Server. If necessary, contact your Opsware administrator for the hostname of the Media Server.

Before you perform the tasks to set up OS provisioning, you must have a licensed copy of the OS installation media, which typically comes as a CD-ROM or DVD.

You must know what locations were specified for the OS media. When Opsware SAS was installed, the Opsware Installer prompted for the pathnames of the root directories for the Windows, Solaris, and Linux OS media on the Opsware Media Server. If necessary, contact your Opsware administrator for this information.

Perform the following tasks to set up OS provisioning:

1. On the Media Server host, create the directory structure for the versions of the OS that you plan to use for server provisioning.

   Create the directory structure based on the root directories specified for the OS media during Opsware SAS installation. If necessary, contact your Opsware administrator for the locations of the OS media root directories.

2. The media for each OS that you want to provision needs to be available on the Media Server.

   - For Microsoft Windows, copy the OS media files to the correct location on the Media Server.
   - For Linux, copy the OS media files to the correct location specified on the Media Server. The OS media needs to be NFS exported read write.

     For SUSE Linux, see http://www.suse.de/~nashif/autoinstall/multiplesource.html for information on how to deal with multiple sources.
   - For Sun Solaris, use the Sun Solaris scripts included on the CD-ROM or DVD to copy the OS media files to the correct location on the Media Server.

Creating an MRL with the Import Media Tool

Perform the following steps to create an MRL with the Import Media Tool:

1. Login to the Software Repository host as root.
2. For Sun Solaris and Linux media, NFS mount the OS media on the Media Server from the Software Repository host.

You must know the correct location for the OS media.

For example, enter the following command to NFS mount Solaris and Linux media:

```
theword# mount mediaserver:/usr/local/solaris/5.8 /mnt
```

3 On the Software Repository host, run the `import_media` script in the following directory:

```
/cust/usr/blackshadow/mm_wordbot/util/
```

✓ To write-protect the Windows media share, a password was set for the root user (parameter: `media_server.windows_share_password`) when Opsware SAS was installed. The Opsware Import Media Tool prompts for the password each time you run it. Contact your Opsware administrator for this password.

When running the `import_media` script, specify as an argument the directory where the OS media is mounted. For Windows, you must specify the directory of the Windows OS media by using UNC style with the following syntax:

```
//<server_name>/<sharename>/I386
```

The path must end at the `/I386` directory.

For Windows, the Media Server directory where the OS media is mounted must meet the conventions for a FAT file system. The directory name can consist of any combination (up to eight characters) of letters, digits, or the following special characters: $ % Ã,Â‘ – _ @ { } ~ ` ! # ( ) The directory name can also have an extension (up to three characters) of any combination of letters, digits, or the previously listed special characters. The extension is preceded by a period.

For example, enter the following Import Media tool command for Solaris and Linux:

```
theword# /cust/usr/blackshadow/mm_wordbot/util/import_media
/mnt
```

For example, enter the following Import Media tool command for Windows:

```
import_media //mediasrv.corp.lionscapital.com/PUB/WIN2000/
SERVER/I386
```

Running the Import Media tool writes progress to the log file `import_media.log`. The log file is located on the server where you are running the Import Media Tool script in the directory from which you invoke the script.

Editing an MRL

Perform the following steps to edit an MRL:

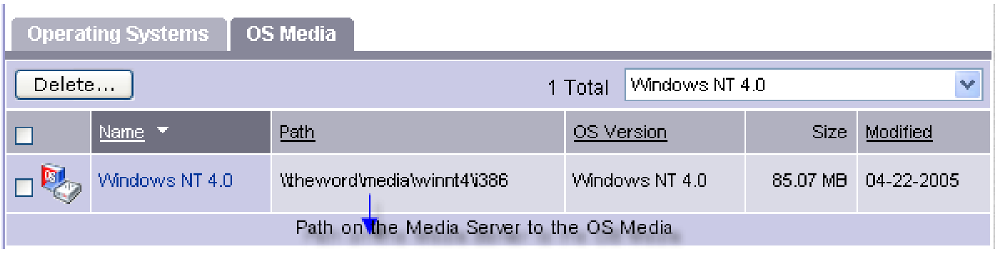
1. Login to the Opsware Command Center. The Opsware Command Center home page appears.

2. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.

3. Click the OS Media tab. A list of Media Resource Locators appears.

   Each MRL represents media available for installation. See Figure 5-1.

Figure 5-1: OS Media Page in the Opsware Command Center



1 Total

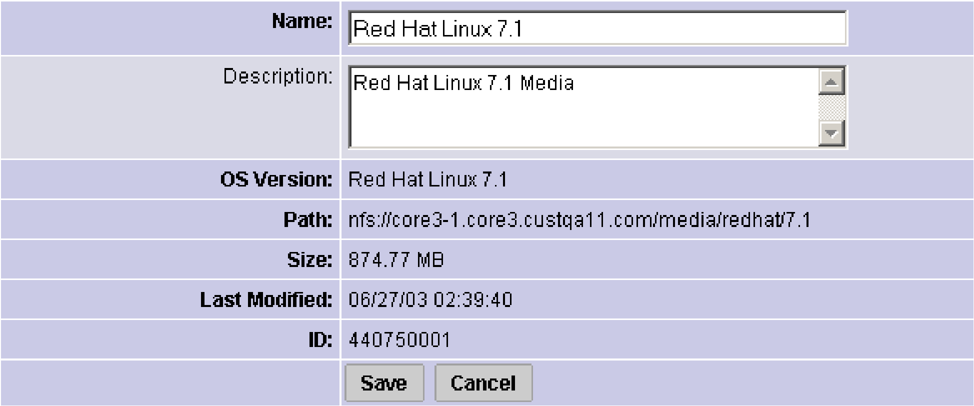
Windows NT 4.0

☐		Name	Path	OS Version	Size	Modified
☐		Windows NT 4.0	\theword\media\winnt4\i386	Windows NT 4.0	85.07 MB	04-22-2005

Path on the Media Server to the OS Media

4. Click the display name for the MRL that you want to edit. The Edit OS Media page appears, as Figure 5-2 shows.

Figure 5-2: Edit OS Media Page in the Opsware Command Center



Name:	Red Hat Linux 7.1
Description:	Red Hat Linux 7.1 Media
OS Version:	Red Hat Linux 7.1
Path:	nfs://core3-1.core3.custqa11.com/media/redhat/7.1
Size:	874.77 MB
Last Modified:	06/27/03 02:39:40
ID:	440750001

5. Modify the name or description of the MRL.

   You cannot edit the OS media path with the Opsware Command Center. If the path for the OS media changes on the Media Server, create a new MRL with the Import Media tool. Then delete the out-of-date MRL by using the Opsware Command Center.

   See “Creating an MRL with the Import Media Tool” on page 103 in this chapter for more information.

6. Click the Save button.

Deleting an MRL

You cannot delete an MRL with the Opsware Command Center when the MRL is specified in an OS definition. To delete an MRL specified in an OS definition, you must first delete the OS definition or specify another MRL in the OS definition.

See “Defining an Operating System” on page 129 in this chapter for more information.

Perform the following steps to delete an MRL:

1. Login to the Opsware Command Center. The Opsware Command Center home page appears.
2. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.
3. Click the OS Media tab. The list of media available for installation appears.
4. Select the OS Media that you want to delete.
5. Click the Delete button. (If the MRL is specified in an OS definition, a warning message appears.)

   The list of Media Resource Locators re-appears.

Additional Windows NT Media Setup Tasks

You must modify the Windows NT media from the vendor before you can use it to provision servers. Perform the following tasks to set up OS provisioning for Windows NT:

- Setting Up Installation of Service Pack 6a
- Applying Microsoft Patch Q143473 to the Windows NT Media

Setting Up Installation of Service Pack 6a

Before you provision Windows NT servers, you must set up the OS Provisioning feature to install Service Pack 6a with the OS. Use the `cmdlines.txt` feature of Windows setup to install Service Pack 6a along with the setup.

Perform the following steps to set up installation of Service Pack 6a:

1. Obtain the Service Pack 6a executable file `sp6i386.exe` from the Microsoft FTP site that contains product updates and copy the file `sp6i386.exe` into the Windows NT `I386\$OEM$` directory on the Media Server.
2. Create a file named `cmdlines.txt` in the `I386\$OEM$` directory that has the following contents:

```
[Commands]
"sp6i386.exe -u -o -z -q"
```

By performing these tasks, Service Pack 6a is silently installed on servers during Windows setup.

For more information about how to install Service Pack 6a with `cmdlines.txt`, see the Microsoft Knowledge Base Article 168814, Installation Option 3, on the Microsoft Web site.

Applying Microsoft Patch Q143473 to the Windows NT Media

Before you provision Windows NT servers, you must apply Microsoft Patch Q143473 to the Windows NT media that you copied to the Media Server.

Without the patch, Windows NT unattended setup stops and prompts you to press any key to shut down. The Windows NT media requires this patch for unattended builds to function properly.

Perform the following steps to apply Microsoft Patch Q143473:

1. Download the patch Q143473 from the Microsoft FTP site that contains patches.
2. Copy the file into the Windows NT `I386\$OEM$` directory on the Media Server.

For more information about applying patch Q143473 to the Windows NT media, see the Microsoft Knowledge Base Article Q143473 on the Microsoft Web site.

Operating System Definitions

This section provides information on operating system definitions within Opsware SAS and contains the following topics:

- Overview of Operating System Definitions
- About Specifying Software in OS Definitions
- About Configuration Files
- About Sun Solaris Profiles
- About Red Hat Linux Configuration Files
- About Microsoft Windows Response Files
- About Microsoft Windows Response Files
- Sample Response File for Windows 2000
- Sample Response File for Windows NT

Overview of Operating System Definitions

To provision a server with an OS, the OS must first be defined in the OS Provisioning feature.

See “Process for Setting up OS Provisioning” on page 95 in this chapter for information about the overall process of setting up OS provisioning.

OS definitions store all relevant information needed to provision an OS. You create OS definitions by using the Prepare Operating System Wizard in the Opsware Command Center.

Perform the following tasks to define an OS:

- Specify properties for the OS
- Specify the OS media from which to perform the installation by selecting an MRL

  See “OS Media Management” on page 101 in this chapter for information about MRLs.
- Upload the following installation resources used during unattended installation:
  - A standard configuration file for the OS

    See “About Configuration Files” on page 110 in this chapter for more information.

- A build customization script, which can modify the installation process at certain points

  See “Build Customization Scripts” on page 115 in this chapter for more information.

- For Microsoft Windows only, a Hardware Signature, which contains hardware specific information

  See “About Hardware Signature Files for Windows” on page 128 in this chapter for more information.

Table 5-1 compares the installation resources across operating systems.

Table 5-1: Installation Resources for OS Definitions

INSTALLATION RESOURCE	WINDOWS	SOLARIS	LINUX
Configuration File	Required File name: `unattend.txt`	Required `profile`	Required `profile`
Build Customization Script	Optional Executable file: `run.bat`	Optional Executable file: `run`	Optional Executable file: `run`
Hardware Signature File	Optional *`filename`*`.txt`	Not required	Not required

The configuration file that you upload for each OS can have any filename. When the file is uploaded, the OS Provisioning feature renames the file so that it has the correct name for that OS.

You can edit an OS definition later to add support for new hardware or to change the way the OS is installed.

See “About Editing OS Definitions” on page 133 in this chapter for more information.

About Specifying Software in OS Definitions

Solaris and Linux are package-oriented operating systems. In other words, you can define a particular OS build as a set of Solaris or RPM packages.

An OS definition can contain a list of packages or clusters to install after the base OS installation is complete. You specify the packages to install during OS provisioning in the following ways:

- Uploading a configuration file that specifies to the vendor installation program what software packages to install

  For example, a JumpStart profile contains a list of clusters (and optionally packages) to be installed by JumpStart. A Kickstart configuration file specifies to Kickstart the RPMs to be installed. When you upload a configuration file, the OS Provisioning feature extracts the list of packages that will be installed by the vendor's installer.

  Extracting the packages allows Opsware SAS to manage the software so that you can upgrade or remove software from an OS definition later.

- By adding packages directly to an OS definition

  You can select packages from the list of packages already uploaded to Opsware SAS. The Opsware Agent installs the selected packages after the vendor installation program installs the initial OS and the packages specified in the configuration file.

About Configuration Files

A configuration file is required for each OS definition:

- For Solaris, you must create and upload a JumpStart profile.
- For Red Hat Linux, you must create and upload a Kickstart configuration file.
- For SUSE Linux, you must upload a YaST2 configuration file.
- For Windows, you must create and upload a response file.

The purpose of these configuration files is described in the following topics.

About Sun Solaris Profiles

When preparing a Solaris OS definition, the OS Provisioning feature requires that you upload a JumpStart profile. The OS Provisioning feature extracts the list of software to be installed from the uploaded profile by examining the cluster and package specifications. If the profile specifies an invalid cluster or package name, the OS Provisioning feature generates an error. No other profile validation occurs when the profile is uploaded.

The Solaris profile must meet the following requirements:

- Be a valid profile that you would use with a JumpStart server

- Specify that the installation type is an initial installation and not an upgrade
- Specify a package-based installation by listing the clusters and packages to install
- Specify disk partitioning information

See "About Conditional Packages for Solaris" on page 128 in this chapter for information about how the OS Provisioning feature handles Solaris conditional packages.

About Red Hat Linux Configuration Files

The Red Hat Linux configuration file instructs the Kickstart server on what packages to install, how to partition the drive, and how to configure the runtime network post-installation.

When preparing a Red Hat Linux OS definition, Opsware SAS validates the Kickstart configuration file. When the configuration file is uploaded, the OS Provisioning feature parses the file in order to extract the package list.

The Red Hat Linux configuration file must meet the following requirements:

- Be a valid configuration file that you would use with a Kickstart server
- Specify the RPM packages to install
- Must include the reboot option

In the Red Hat Linux configuration file, do not enable firewalls. The Opsware Agent must communicate with Opsware SAS on port 1002.

About SUSE Linux Configuration Files

The SUSE Linux configuration file instructs YaST2 on what packages to install, how to partition the drive, and how to configure the resulting machine.

When preparing a SUSE Linux OS definition, Opsware SAS validates the YaST2 configuration file. When the configuration file is uploaded, the OS Provisioning feature parses the file in order to extract the package list.

The SUSE Linux configuration file must meet the following requirements:

- Be a valid YaST2 configuration file
- Under the general options, the reboot and confirm properties in the mode resource needs to be set to true and false respectively

For SUSE Linux, see http://www.suse.de/~nashif/autoinstall/8.0/html/index.html and http://www.suse.de/~nashif/autoinstall/sles8/html/index.html for information on Linux installations.

About Microsoft Windows Response Files

For a Windows OS definition, the configuration file must meet the following requirements.

- Be an unattended installation response file that contains the following settings:
  - Sets the `OemPreInstall` key to yes. If this key is not set, the OS Provisioning feature will set it automatically.
  - Specifies a network configuration so that the OS boots for the first time with a valid IP address.
  - Suppresses any dialog boxes that might appear during the Text and GUI mode portions of Windows setup.

When uploading an `unattend.txt` file, Opsware SAS validates the response file and rejects incomplete response files.

See “Sample Response File for Windows 2000” on page 112 in this chapter for information about examples of valid Windows response files. See “Sample Response File for Windows NT” on page 113 in this chapter for information about examples of valid Windows response files.

Sample Response File for Windows 2000

The following sample response file shows how to create a valid response file for a Windows 2000 installation. This sample response file contains the required settings for Windows 2000 provisioning with the OS Provisioning feature.

```
; Minimal unattend.txt for installing Windows 2000 Professional,
; Server, and Advanced Server
;
; All parameters listed in this file are required for Windows
; 2000 setup and Opsware OS provisioning to be completely
; unattended.
;
; Values between <> are values that you must provide.
; For more information, see the unattend.doc file in the
; Support\Tools folder in the Deploy.cab file on the Windows
; 2000 CD-ROM.
;
```

```
[Unattended]
UnattendMode=FullUnattended
TargetPath=*
OemSkipEula=Yes
; The OemPreInstall key is automatically provided by Opsware
; OS provisioning.
OemPreinstall=Yes

[GuiUnattended]
AdminPassword=<*>
OEMSkipRegional=1
OEMSkipWelcome=1
TimeZone=<085>

[UserData]
; The ComputerName parameter is automatically provided by
; Opsware OS provisioning.
ComputerName=*
FullName=<Your User Name>
OrgName=<Your organization name>
ProductID=<License key provided by Microsoft>

; For server installs only
[LicenseFilePrintData]
AutoMode = <PerServer>
AutoUsers = <5>

; Installs TCP/IP on network interfaces. Interfaces are
; configured for DHCP.
[Networking]

[Identification]
JoinWorkgroup = <Workgroup>
```

Sample Response File for Windows NT

The following sample response file shows how to create a valid response file for a Windows NT installation. This sample response file contains the required settings for Windows NT provisioning with the OS Provisioning feature.

```
; Minimal unattend.txt for installing Windows NT Workstation,
; Server, and Enterprise Server.
;
; All parameters listed in this file are required for Windows NT
; setup and Opsware OS provisioning to be completely unattended.
```

```
;
; Values between <> are values that you must provide.

[Unattended]
ConfirmHardware = no
TargetPath = *
NoWaitAfterTextMode = 1
NoWaitAfterGuiMode = 1
OEMSkipEula = yes

; The OemPreInstall key is automatically provided by Opsware
; OS provisioning.
OemPreinstall = yes

[UserData]
; The ComputerName parameter is automatically provided by
; Opsware OS provisioning.
ComputerName = *
FullName=<Your User Name>
OrgName=<Your organization name>
ProductID=<License key provided by Microsoft>

; For server installs only
[LicenseFilePrintData]
AutoMode = <PerServer>
AutoUsers = <5>

[GuiUnattended]
AdvServerType = <SERVERNT>
OEMSkipWelcome = 1
OEMBlankAdminPassword = 1
TimeZone = <"(GMT) Monrovia, Casablanca">

[Display]
ConfigureAtLogon = 0
BitsPerPel = 16
XResolution = 1024
YResolution = 768
VRefresh = 70
AutoConfirm = 1

; Installs TCP/IP on network interfaces. Interfaces are
; configured for DHCP.
[Network]
JoinWorkgroup = <Workgroup>
DetectAdapters = ""
InstallProtocols = ProtocolsSection
```

```
[ProtocolsSection]
TC = TCParameters

[TCParameters]
DHCP = Yes
```

Build Customization Scripts

This section provides information on build customization scripts within Opsware SAS and contains the following topics:

- Overview of Build Customization Scripts
- Sun Solaris Build Process
- About the Solaris Build Customization Script
- Solaris Provisioning and NFS on the Boot Server
- Requirements for Solaris Build Customization Scripts
- Sample Solaris Build Customization Script
- Linux Build Process
- About Linux Build Customization Scripts
- Requirements for Linux Build Customization Scripts
- Microsoft Windows Build Process
- About Windows Build Customization Scripts

Overview of Build Customization Scripts

To control the way each OS is installed on servers, the OS Provisioning feature utilizes OS-specific build scripts. Build scripts manage each OS installation from the point where bare-metal hardware is connected to the network and booted for the first time through the point where the OS and an Opsware Agent are installed on the server.

Customers need flexibility to customize how operating systems are installed in their environments. Therefore, the OS provisioning build scripts provide hooks into the build process to modify OS installations at specific points. These hooks call a single build customization script at the appropriate time in the OS installation process. Examples of what you can customize by using build customization scripts are given in the following topics.

Because each build script is specific to the OS it installs, how to create a build customization script varies by OS. Additionally, the way a build customization script can modify the OS installation process varies by OS.

To use a build customization script, follow this general process:

1. Upload the file that contains the build customization script (with the correct filename) in the Opsware Command Center by clicking Software ➤ Packages in the navigation panel. (The build script for an OS looks for a build customization script that has a specific name.) When you upload the file, specify “Installation Hooks” as the type of package.

   See “Uploading a Package” on page 211 in Chapter 7 for more information.

2. While preparing an OS definition with the wizard, select the build customization script during Step 2 (Define Installation). The uploaded build customization scripts appear in a list when you click the Select button.

   See “Defining an Operating System” on page 129 in this chapter for more information.

Sun Solaris Build Process

The following table describes in detail the exact steps that occur in the OS Provisioning feature to provision an installation client with Solaris.

A user initiates the build process with Steps 1 and 5. The rest of the build process steps happen automatically in the OS Provisioning feature.

It is important to understand the Solaris build process before you include a build customization script in a Solaris OS definition. See Table 5-2.

Table 5-2: Sun Solaris Build Process

PHASE	BUILD PROCESS STEPS
Pre-installation	1 A user boots the installation client over the network by entering the command in a console attached to the server: `boot net:dhcp - install` 2 The installation client boots from the network by using a provided Solaris 9 JumpStart miniroot (included as part of the OS Provisioning feature), eventually running a JumpStart `begin` script. The `begin` script is used to start the Opsware OS Build Agent. 3 The OS Build Agent registers with the OS Build Manager. 4 The Solaris `build` script probes the hardware configuration of the installation client and registers it with Opsware SAS. The installation client then appears in the Server Pool list in the Opsware Command Center.

Table 5-2: Sun Solaris Build Process

PHASE	BUILD PROCESS STEPS

Phase One	5 In the Opsware Command Center, a user chooses to install an OS on an available installation client.
	6 The Solaris build script mounts the Solaris installation media indicated by the MRL in the OS definition that the user selected.
	7 The Solaris build script retrieves the profile associated with the selected OS definition and copies it to `$SI_PROFILE`, the standard JumpStart location for dynamic JumpStart profiles.
	8 The Solaris build script executes the build customization script:
	`/sbin/sh run Pre-JumpStart`
	9 The Solaris build script validates the profile by using the JumpStart installer (`pfinstall`) in ted mode.
	10 The Solaris build script causes the OS Build Agent to run in the background, allowing the JumpStart `begin` script to complete.
	11 The JumpStart installer `pfinstall` is invoked by the JumpStart installer script and Solaris is installed. Concurrently, the OS Build Agent monitors the installation process. Feedback is displayed in the Opsware Command Center.
	12 The JumpStart installer `pfinstall` completes and runs the JumpStart `finish` script, which indicates to the OS Provisioning feature that the OS installation is complete.
	13 The build script executes the build customization script a second time:
	`/sbin/sh run Post-JumpStart`
	14 The installation client reboots.

Table 5-2: Sun Solaris Build Process

PHASE	BUILD PROCESS STEPS

Phase Two	15 On entering multiuser mode, the OS Build Agent is invoked and it contacts the OS Build Manager.
	16 The Solaris build script executes the build customization script:
	`/sbin/sh run Pre-Agent`
	17 The Solaris build script installs the Opsware Agent.
	18 The Solaris build script executes the build customization script:
	`/sbin/sh run Post-Agent`
	19 The Solaris build script exits and Phase Two finishes.

The OS Provisioning feature takes over, causing a reconcile of the selected software to be installed onto the installation client.

See the *Opsware® SAS 5.2 User's Guide* for more information about how reconcile works to install software on servers.

Solaris Provisioning and NFS on the Boot Server

If you want to provision a Solaris server and the Opsware Boot Server is on a Redhat server, you must disable NFS v3 on the Boot Server. (If the Boot Server is on a Solaris server, do not perform this action.) To disable NFS v3, perform the following steps:

1 On the Boot Server host, create the following file:

```
/etc/sysconfig/nfs
```

2 In the newly created `nfs` file, add the following line:

```
MOUNTD_NFS_V3=no
```

3 Restart NFS:

```
/etc/init.d/nfs stop
/etc/init.d/nfs start
```

About the Solaris Build Customization Script

You can customize a Solaris installation at multiple points; therefore, the Solaris build customization script runs more than once:

- A pre-installation hook for the first stage (Pre-JumpStart)

  During phase one, the build customization script runs in the JumpStart environment. The script can use all the standard JumpStart environment variables, such as `SI_PROFILE`. All the environment variables associated with the standard JumpStart probe keywords and values are set (for example, `SI_DISKLIST`, `SI_HOSTADDRESS`, and `SI_MEMSIZE`).

  When the `run` script is invoked at the Pre-JumpStart point, it can perform any actions that a JumpStart `begin` script would perform. For example, the script could modify the downloaded profile before the OS installation begins. At this point, the Solaris profile is downloaded from the OS Provisioning feature but the profile has not been passed to the JumpStart server.

  For the complete list of the environment variables, see the *Solaris 9 Installation Guide*.

- A post-installation hook for the first stage (Post-JumpStart)

  When the `run` script is invoked at the Post-JumpStart point, it can perform any actions that a JumpStart `finish` script would perform. One example would be to set custom `eeprom` settings. The installation client's file systems are available for modification at this point and are mounted on the `/a` partition for the `finish` script environment.

- A pre-installation hook for the second stage (Pre-Agent)
- A post-installation hook for the second stage (Post-Agent)

  During Phase Two, the `run` script is executed after the installation client has rebooted, at a point after the system is up and running in multi-user mode with most services started.

The last 4K of output produced by the build customization script (`stdout` and `stderr`) appears in the Opsware Command Center output details for the OS.

Requirements for Solaris Build Customization Scripts

To use a build customization script for Solaris, you must meet the following requirements:

- Create the script as a Bourne shell script and name it `run`.
- Include the `run` script in an archive file in `tar.Z` format. Include the script at the top level of the archive. During OS provisioning, the `tar.Z` archive is unpacked on the installation client and the script is processed by `/sbin/sh`.
- The `run` script is unpacked in its own directory with the other files in the archive. This directory serves as the current working directory when the `run` script is invoked. Based

on this fact, correctly refer to the other files in the archive. For example, unpacking and invoking the `run` script follows this general process:

```
mkdir /var/tmp/inst_hook
cd /var/tmp/inst_hook
zcat hook.tar.Z | tar xf -
/sbin/sh run <stage>
```

- The script cannot cause the installation client to drop its network connection (for example, do not use the script to reboot the installation client or reconfigure the active network interface). If the installation client drops its network connection, the OS provisioning process will fail.
- The `run` script must exit normally. If the script exits with a non-zero value, the OS provisioning process will end. However, the JumpStart process will continue when a pre-installation hook fails (exits with a non-zero value). When creating the run script, you should ensure that the JumpStart process does not continue when a pre-installation hook fails.
- The `run` script should not take an exceptionally long time to complete, otherwise the OS provisioning process might time out.

Sample Solaris Build Customization Script

```
#!/sbin/sh
pre_jumpstart() {

    #

    # strip any partitioning information out of profile, and
    # replace it with keywords to use default partitioning, but
    # to size swap equal to the amount of physical RAM

    #

cat $SI_PROFILE | grep -v partitioning | grep -v filesys > /tmp/
profile.$$

    echo "partitioning default" >> /tmp/profile.$$

    echo "filesys any $SI_MEMSIZE swap" >> /tmp/profile.$$

    cp /tmp/profile.$$ $SI_PROFILE

    rm -f /tmp/profile.$$

}
post_jumpstart() {
    #
    # set local-mac-address eeprom setting
    #
    eeprom 'local-mac-address?=true'
}
pre_agent() {
    : # do nothing
}
post_agent() {
    : # do nothing
}
case "$1" in
          Pre-JumpStart)  pre_jumpstart ;;
          Post-JumpStart) post_jumpstart ;;
          Pre-Agent)      pre_agent ;;
          Post-Agent)     post_agent ;;
esac
```

Linux Build Process

The following table describes in detail the exact steps that occur in the OS Provisioning feature to provision an installation client with Red Hat or SUSE Linux.

A user initiates the build process with Steps 1 and 6. The rest of the build process steps happen automatically in the OS Provisioning feature.

It is important to understand the Linux build process before you include a build customization script in a Linux OS definition. See Table 5-3.

Table 5-3: Linux Build Process

PHASE	BUILD PROCESS STEPS
Pre-installation	1 A user boots the installation client from PXE or the Linux Boot CD ROM. 2 The installation client loads a custom Red Hat AS 3.0 boot image and mounts the second stage image specified by the kernel parameters. 3 Anaconda is replaced by a custom Opsware script that is used to invoke the OS Build Agent. 4 The OS Build Agent registers with the Opsware Build Manager. 5 The Linux build script probes the hardware configuration of the installation client and registers it with Opsware SAS, causing the installation client to appear in the Server Pool list in the Opsware Command Center.
Phase One	6 In the Opsware Command Center, a user selects the target version of Linux to install on the installation client. 7 The Linux build script creates a 10 cylinder partition at the beginning of the disk and copies the target boot image from the Boot Server to this partition. 8 The Linux build script copies GRUB onto the partition and installs it into the MBR. 9 The Linux build script configures GRUB to boot this partition and kernel arguments are set to do an NFS installation on the location indicated by the MRL. 10 If the Custom Attribute `kernel_arguments` is set for the OS definition, these kernel arguments are appended. 11 The OS Build Agent exits and the server reboots.

Table 5-3: Linux Build Process

PHASE	BUILD PROCESS STEPS
Phase Two	**12** The target boot image loads and runs the OS Build Agent. **13** The Linux build script verifies that the media indicated by the MRL is the same version as the boot image under which it is running. **14** The Linux build script writes the configuration file defined by the MRL to the disk. **15** If it exists, the Linux build script runs the build customization script. **16** The Linux build script runs in the background. The OS Build Agent and Anaconda starts. The Linux installation starts normally by using the configuration file written to the disk. Concurrently, the OS Build Agent monitors the installation process providing feedback, which is displayed in the Opsware Command Center. **17** After all packages have been installed, as part of the post install, the OS Build Agent copies the Opsware Agent Installer and the OS Build Agent to the server and sets up an `init` script to start the OS Build Agent after the reboot. **18** When the OS installation completes, Anaconda reboots the installation client, which will boot from the newly installed OS.
Phase Three	**19** On entering multi-user mode, the OS Build Agent is invoked and contacts the OS Build Manager. **20** The Linux build script installs the Opsware Agent. **21** The Linux build script exits. The OS installation section of provisioning is complete.

About Linux Build Customization Scripts

The Linux build script runs a single installation hook that gives you the ability to customize the Linux build process before Anaconda loads.

The installation hook is run in a RAM disk right before the installation program runs but after the network has been brought up.

Requirements for Linux Build Customization Scripts

To use a build customization script for Linux, you must meet the following requirements:

- Create an executable script and name it `run`.
- Include the `run` script in an archive file in `tar.gz` format. Include the script at the top level of the archive. During OS provisioning, the `tar.gz` archive is unpacked on the installation client and the script is executed.
- The `run` script is unpacked in its own directory with the other files in the archive. This directory serves as the current working directory when the `run` script is invoked. Based on this fact, correctly refer to the other files in the archive. For example, unpacking and invoking the `run` script follows this general process:

```
mkdir /tmp/installhook
cd /tmp/installhook
tar -xzf hook.tgz
./run 2>&1
```

- The `run` script should not take an exceptionally long time to complete, otherwise the OS provisioning process might time out.
- The `run` script must exit normally. If the script exits with a non-zero value, the OS provisioning process will end.
- The `run` script must have execute permissions to function properly.

Microsoft Windows Build Process

Table 5-4 describes in detail the exact steps that occur in the OS Provisioning feature to provision an installation client with Windows.

A user initiates the build process with Steps 1 and 6. The rest of the build process steps happens automatically in the OS Provisioning feature.

Table 5-4: Microsoft Windows Build Process

PHASE	BUILD PROCESS STEPS
Pre-installation	**1** A user boots an installation client over the network by using a PXE network bootstrap program or by using the Windows Boot Image. **2** The user selects `Windows` from the boot menu on the console for the PXE network bootstrap program. **3** PXE boots the Windows Opsware OS Build Agent over the network. **4** The Opsware OS Build Agent prompts the user to create a FAT boot partition on which to install Windows. **5** The Opsware OS Build Agent collects pertinent hardware information and registers the information with Opsware SAS. The server is ready to be provisioned and is available for selection from the Server Pool in the Opsware Command Center.
Phase One	**6** The user selects an DOS server from the Server Pool list in the Opsware Command Center and assigns a Windows OS definition or a Windows template to the server. **7** The Windows build script mounts the Windows installation media as indicated by the Media Resource Location (MRL). **8** The Windows build script initiates Windows unattended setup. **9** The Windows build script waits for Windows unattended setup to complete and Windows to boot for the first time.
Phase Two	**10** Windows boots for the first time. **11** If a build customization script was specified in the OS definition, it is executed by the Windows build script. **12** The Windows build script installs the Opsware Agent. The Windows build script exits and Phase Two is complete.

About Windows Build Customization Scripts

The Windows build script includes one installation hook that runs after the Windows OS is installed but before the Opsware Agent is installed on the server.

The installation hook must be packaged as a Microsoft cabinet file. During the provisioning process, the cabinet file is downloaded to the server being provisioned and extracted into a private temporary directory.

The OS Provisioning feature expects to find a file named `run.bat` in the top level directory of the cabinet archive. If the file is found, the OS Provisioning feature executes the `run.bat` file in a command shell and returns the output of the command to the Opsware Command Center.

If running the `run.bat` file returns a non-zero exit code, the OS Provisioning feature detects the failure and ends the build process for that server.

A customer can use the hook as an opportunity to perform common post OS-installation tasks for Windows, such as modifying the Windows registry or applying security templates.

Working with OS Definitions

This section provides information on OS definitions within Opsware SAS and contains the following topics:

- About Conditional Packages for Solaris
- Overview of Installation Order for Solaris and Linux
- About Hardware Signature Files for Windows
- Defining an Operating System
- About Editing OS Definitions
- Changing the Properties for an OS Definition
- Modifying the Way an OS Is Installed on Servers
- Modifying Which Packages an OS Definition Installs
- Viewing the History of Changes for an OS Definition
- Deleting an OS Definition

About Conditional Packages for Solaris

A metacluster specified in a JumpStart profile can include conditional packages. Conditional packages are packages that the Solaris installation program might (or might not) install during JumpStart. The Solaris installation program determines which packages to install based on the hardware attributes of the server being provisioned. For example, the presence of a specific graphics card would cause the drivers for that card to be installed.

When you upload a Solaris profile in the Prepare Operating System Wizard, the OS Provisioning feature extracts the list of packages specified in the profile and displays them on the Review Packages page. The Review Packages page does not display Solaris conditional packages because Opsware SAS cannot determine, at that time, whether the conditional packages will be installed.

You can specify to always install conditional packages by adding them to the Packages List. Adding packages to the Packages List does not change the Solaris profile. Opsware SAS installs the packages even if the JumpStart Installer does not install them.

See “Defining an Operating System” on page 129 in this chapter for more information. See “About Editing OS Definitions” on page 133 in this chapter for information about adding packages to or removing packages from the Packages List.

Overview of Installation Order for Solaris and Linux

For Sun Solaris, Red Hat Linux, and SUSE Linux, installation order is defined by the vendor. These dependencies control the order that packages are installed during JumpStart, Kickstart, and YaST2.

However, the Opsware Command Center provides the ability to specify additional OS packages to install on servers after JumpStart, Kickstart, or YaST2 completes. You can specify installation order for these additional packages. You set the package installation order when you define the OS.

See “Defining an Operating System” on page 129 in this chapter for information about how to specify the installation order while reviewing packages in the Prepare Operating System Wizard.

About Hardware Signature Files for Windows

A Windows response file contains information that is applicable to any hardware make and model. The remaining part of the configuration file is hardware-specific, taking into account differences between specific models of servers.

The generic part of the response file specifies how to install and configure the Windows OS. Typically, the hardware-specific part specifies hardware dependent configuration for devices such as mass storage.

Based on the hardware you expect to provision, you can upload hardware-specific files for each Windows OS definition. You map a signature for that hardware to the correct hardware-specific profile. The OS Provisioning feature selects the correct Hardware Signature file at build time based on the hardware signature of the server that is about to be provisioned.

Certain x86-processor-based hardware requires pre-installation configuration of the OS. You usually perform this configuration by running vendor-supplied utilities with certain parameters. Because the utilities are hardware specific, you can script these configuration steps by using a Hardware Signature file.

Utilities referenced by the Hardware Signature file must be accessible through the network during build time.

> Using Hardware Signatures is not required for Sun Solaris or Red Hat Linux operating systems because Solaris and Linux distributions do not need to be tailored for particular hardware models.

Defining an Operating System

The Prepare Operating System Wizard helps you define an OS installation that you can use during the OS provisioning process.

Perform the following steps to define an operating system:

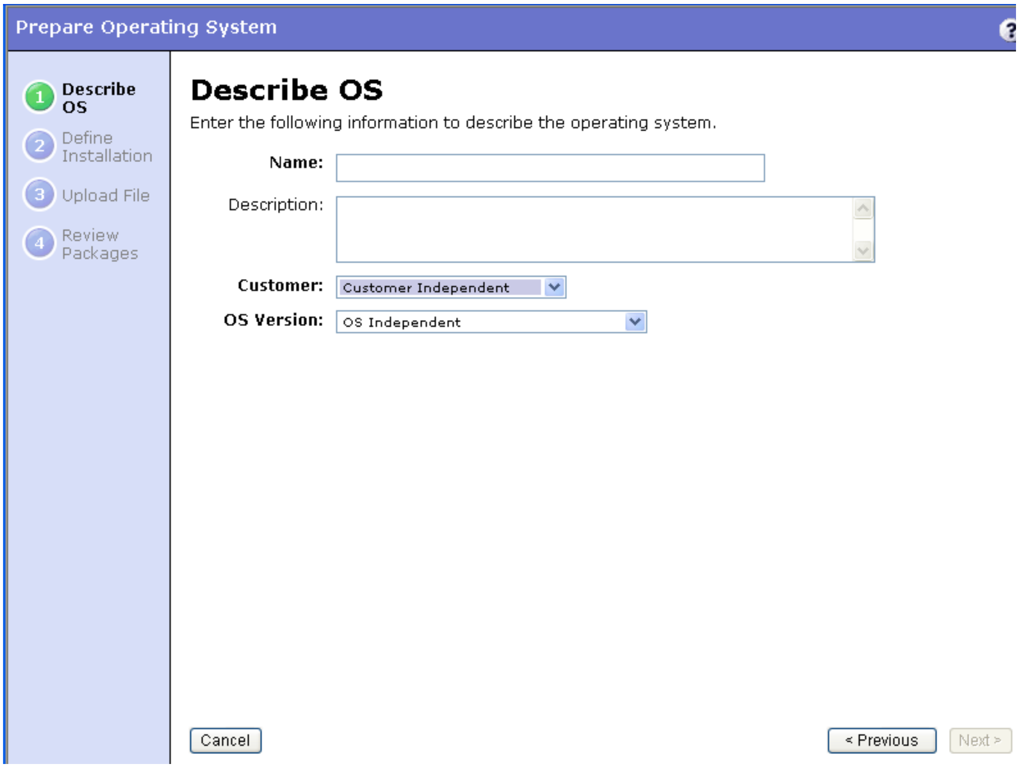
1. From the Opsware Command Center home page, click the Prepare OS link in the Tasks panel.

   Or

   From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears. Click the Prepare OS button.

The Describe OS page appears, as Figure 5-3 shows.

Figure 5-3: Describe OS Page in the Prepare Operating System Wizard



Prepare Operating System

Describe OS

Enter the following information to describe the operating system.

Name:

Description:

Customer: Customer Independent

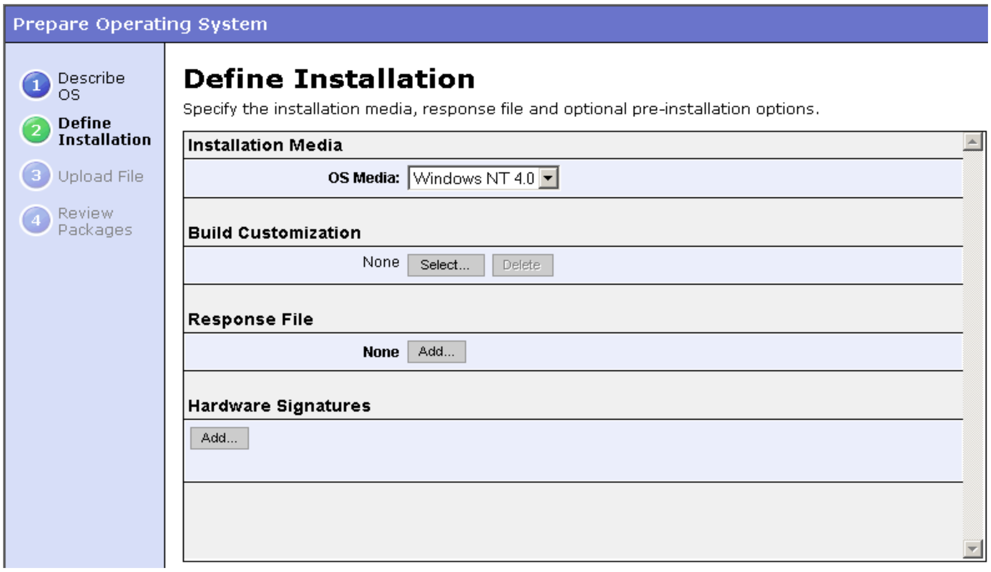
OS Version: OS Independent

2 Describe the OS by specifying the following information:

- **(Required)** Name – sets the display name for the OS.
- **(Required)** Customer – associates the OS with a specific customer; to set up the OS for use by all customers, select Customer Independent.
- **(Required)** OS Version – sets the version of the OS (selected from the pre-populated list of the operating systems that Opsware SAS supports).
- (Optional) Description – provides a long text description; using the description to identify the platform and hardware support is recommended.

3 Click the Next button. The Define Installation page appears, as Figure 5-4 shows.

Figure 5-4: Define Installation Page in the Prepare Operating System Wizard



Prepare Operating System

Define Installation

Specify the installation media, response file and optional pre-installation options.

Installation Media

OS Media: Windows NT 4.0

Build Customization

None Select... Delete

Response File

None Add...

Hardware Signatures

Add...

4 Define the installation by specifying the following information:

- **(Required)** OS Media – sets the MRL for the OS (select one MRL from the pre-populated drop-down list).

  See "OS Media Management" on page 101 in this chapter for information about how to set up OS media so that the MRL for the media appears in the drop-down list.

- **(Required)** A configuration file – indicates a JumpStart profile, Kickstart configuration file, YaST2 `autoinst.xml` file, or Windows response file to upload into the OS Provisioning feature.

  The file that you upload can have any filename. However, the OS Provisioning feature renames the file with the correct filename for use by the vendor installation program.

- (Optional – Windows only) Hardware Signatures – defines the list of hardware that the OS supports.

  Click the Add button to open the Add Hardware Signature Setting window. The Applies To field is pre-populated with the hardware makes and models that have been successfully built so that they appear in the Managed Server list.

You can add multiple Hardware Signature files to a Windows OS definition.

- (Optional) Build Customization Script – customizes the way the build process operates for that OS (select a file from the popup window).

  The way you can customize the build process is specific to each build script. You must follow the requirements for build customization scripts to use this feature. Scripts appear in the popup window after you upload them through the Opsware Command Center.

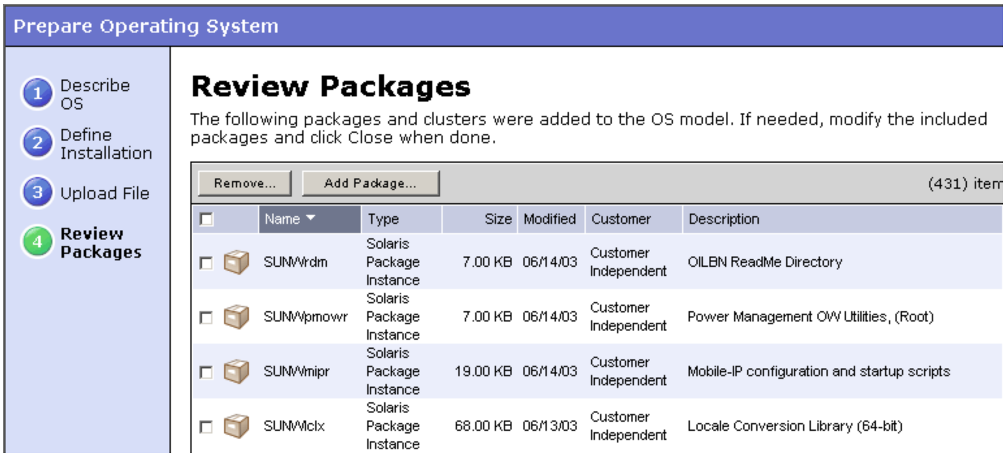
  See "Build Customization Scripts" on page 115 in this chapter for more information.

5 Click the Upload button.

Opsware SAS creates the OS definition and uploads the configuration file (and parses packages for Sun Solaris and Red Hat and SUSE Linux). A progress bar appears that shows the progress of the OS preparation process.

6 Click the Next button to review the packages. A page appears that shows the list of packages, as Figure 5-5 shows.

Figure 5-5: Review Packages Page in the Prepare Operating System Wizard



Review Packages

The following packages and clusters were added to the OS model. If needed, modify the included packages and click Close when done.

(431) item

□	Name	Type	Size	Modified	Customer	Description
□	SUNWrdm	Solaris Package Instance	7.00 KB	06/14/03	Customer Independent	OILBN ReadMe Directory
□	SUNWpmowr	Solaris Package Instance	7.00 KB	06/14/03	Customer Independent	Power Management OW Utilities, (Root)
□	SUNWmipr	Solaris Package Instance	19.00 KB	06/14/03	Customer Independent	Mobile-IP configuration and startup scripts
□	SUNWlclx	Solaris Package Instance	68.00 KB	06/13/03	Customer Independent	Locale Conversion Library (64-bit)

For Solaris and Linux, the list shows the vendor packages that were specified in the Solaris profile or Linux configuration file.

For Windows, the list is empty because you cannot specify specific packages in the Windows response file. You can add packages to the Windows OS definition by clicking the Add Package button.

7 (Optional) Click the Remove or Add Package buttons to modify the list of software that the OS definition installs or to change the installation order.

See “About Conditional Packages for Solaris” on page 128 in this chapter for information about how to ensure Solaris conditional packages are always installed.

8 Click the Close button to end the Wizard.

About Editing OS Definitions

You can edit an OS definition in the following ways:

- By changing the properties for the OS, such as which customer can use the OS definition to provision servers
- By modifying the way that the OS is installed on servers by changing the configuration file or customizing the way the build process works for that OS definition
- By adding custom attributes to the OS definition to override default values in the build process

  See “Default Values for the OS Build Process” on page 138 in this chapter for more information.

  See “Managing Nodes on the Software Tree” on page 255 in Chapter 10 for information about how to set custom attributes for software nodes.
- By modifying which packages are installed with the OS definition

  Modifying the list of packages in an OS definition does not change the configuration file uploaded for the OS definition. Opsware SAS installs the packages after the OS installation technology (Sun Solaris JumpStart, Red Hat Linux Kickstart, or SUSE Linux YaST2) installs the packages specified in the configuration file. For Microsoft Windows, the response file cannot specify specific packages to install; however, you can add Windows packages so that Opsware SAS installs them with the OS.
- By setting up configuration tracking for an OS definition

  See “Configuration Tracking Policies” on page 392 in Chapter 13 for information about how to set a configuration tracking policy for the OS definition.

Changing the Properties for an OS Definition

Perform the following steps to change the properties for an OS definition:

1 From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.

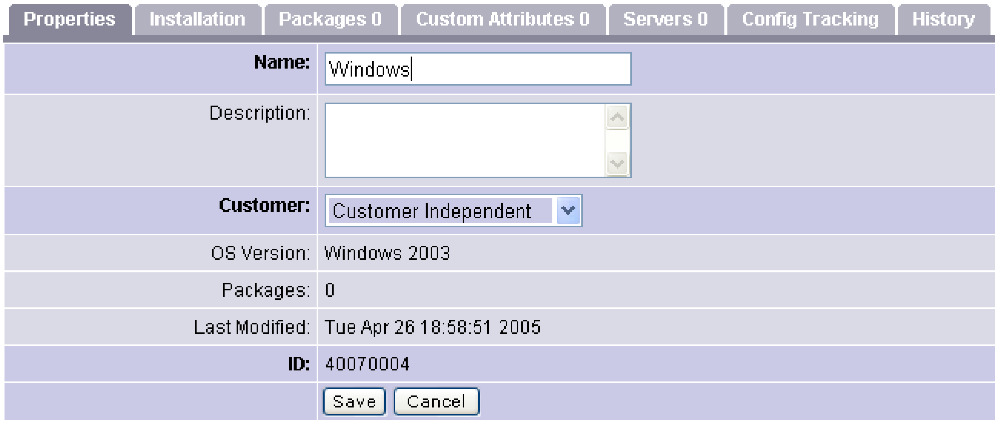
2. Click the display name of the OS that you want to edit. The Edit Operating System page appears.

3. Click the Properties tab (see Figure 5-6) and modify the following settings:

   - Name – sets the display name for the OS.
   - Description – provides a long text description of the OS.
   - Customer – associates the OS with a specific customer.

     If an OS definition is used (a server is provisioned by using the OS definition), you cannot change the customer association for that OS definition.

Figure 5-6: Properties Tab for an OS Definition in the Opsware Command Center



Name:	Windows
Description:	
Customer:	Customer Independent
OS Version:	Windows 2003
Packages:	0
Last Modified:	Tue Apr 26 18:58:51 2005
ID:	40070004

4. Click the Save button.

Modifying the Way an OS Is Installed on Servers

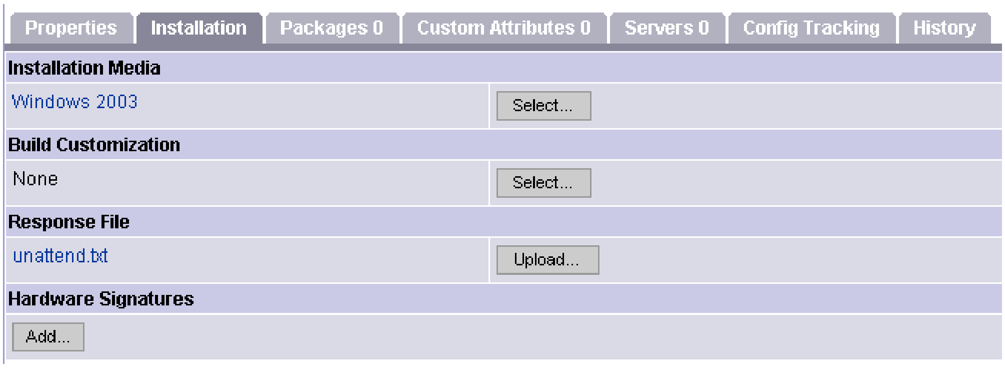
Perform the following steps to modify the way an OS is installed on servers:

1. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.

2. Click the display name of the OS that you want to edit. The Edit Operating System page appears.

3 Click the Installation tab. The installation resources defined for the OS definition appear, as Figure 5-7 shows.

Figure 5-7: Installation Tab for an OS Definition in the Opsware Command Center



Installation Media

Windows 2003 — Select...

Build Customization

None — Select...

Response File

unattend.txt — Upload...

Hardware Signatures

Add...

4 Modify the following settings:

- Installation Media – sets the MRL for the OS. Click the Select button and select an OS media from the list in the popup window.
- Build Customization Script – customizes the way the build process operates for that OS. Click the Select button and select a build customization package from the list in the popup window.

  Scripts appear in the popup window after you upload them through the Opsware Command Center.
- Configuration file – indicates a JumpStart profile, Kickstart configuration file, YaST2 configuration file, or Windows response file to upload into the OS Provisioning feature. Click the Upload button and enter the filename or browse to the file.

  The file that you upload can have any filename. However, the OS Provisioning feature renames the file with the correct filename for use by the vendor installation program.
- Hardware Signatures for Windows *only* – defines the list of hardware that the OS supports. Click the Add button and select the hardware signature that you want to include in the OS definition.

  Hardware signatures appear in the list box after a server with that make and model are successfully built so that it appears in the Managed Server list.

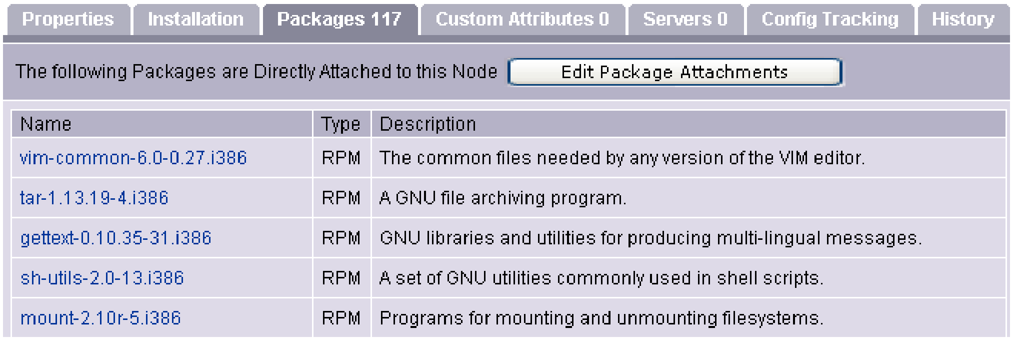
5 Click the Save button.

Modifying Which Packages an OS Definition Installs

Perform the following steps to modify which packages an OS definition installs:

1. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.
2. Click the display name of the OS that you want to edit. The Edit Operating System page appears.
3. Click the Packages tab. The list of packages that the OS definition installs appears, as Figure 5-8 shows.

Figure 5-8: Packages Tab for an OS Definition in the Opsware Command Center



Name	Type	Description
vim-common-6.0-0.27.i386	RPM	The common files needed by any version of the VIM editor.
tar-1.13.19-4.i386	RPM	A GNU file archiving program.
gettext-0.10.35-31.i386	RPM	GNU libraries and utilities for producing multi-lingual messages.
sh-utils-2.0-13.i386	RPM	A set of GNU utilities commonly used in shell scripts.
mount-2.10r-5.i386	RPM	Programs for mounting and unmounting filesystems.

4. Click the Edit Packages button. The Software Directly Attached page appears.
5. To add a package for installation, click the Add Software button and specify or search for the package that you want to add to the list.
6. To remove packages, select them in the list and click the Remove Software button. The packages are deleted from the list in the page but are not actually removed from the OS definition until you click the Save Edits button.
7. To change the order in which the packages are installed on servers, select the package that you want installed in a different order and click the Up or Down arrows.
8. Click the Save Edits button.

Viewing the History of Changes for an OS Definition

By default, the OS Provisioning feature maintains information about the changes to OS definitions for 180 days.

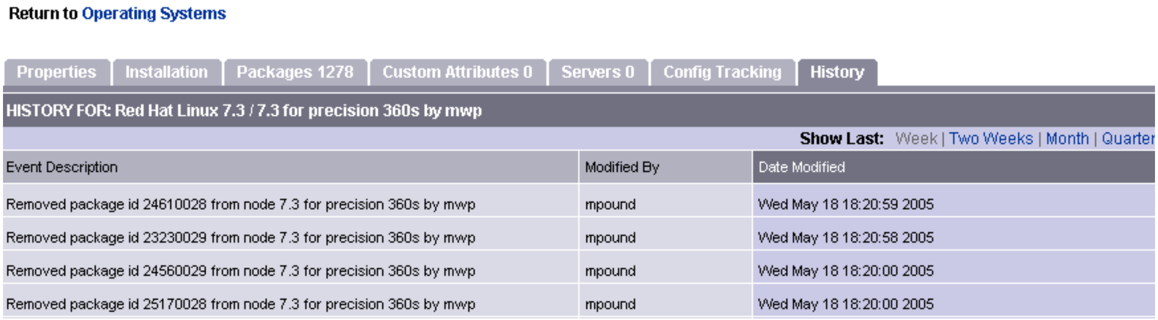
The following actions create an entry in the History tab for an OS definition:

- The customer association is changed for the OS definition.
- A server uses the OS definition to install an OS.
- Packages are added to or removed from the Package List in the OS definition.

Perform the following steps to view the history of changes for an OS definition:

1. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.
2. Click the display name of the OS for which you want to review the history of changes. The Edit Operating System window appears.
3. Click the History tab. The list of events and changes appears, as Figure 5-9 shows.

Figure 5-9: History Tab for an OS Definition in the Opsware Command Center



Return to Operating Systems

HISTORY FOR: Red Hat Linux 7.3 / 7.3 for precision 360s by mwp

Show Last: Week | Two Weeks | Month | Quarter

Event Description	Modified By	Date Modified
Removed package id 24610028 from node 7.3 for precision 360s by mwp	mpound	Wed May 18 18:20:59 2005
Removed package id 23230029 from node 7.3 for precision 360s by mwp	mpound	Wed May 18 18:20:58 2005
Removed package id 24560029 from node 7.3 for precision 360s by mwp	mpound	Wed May 18 18:20:00 2005
Removed package id 25170028 from node 7.3 for precision 360s by mwp	mpound	Wed May 18 18:20:00 2005

Deleting an OS Definition

If a server is using the OS definition or the OS definition is included in a template, you cannot delete it.

Perform the following steps to delete an OS definition:

1. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.
2. Select the OS that you want to delete.
3. Click the Delete button. (If a server has used the OS definition or the OS definition is included in a template, a warning message appears.)

   The list of OS definitions re-appears.

Default Values for the OS Build Process

This section provides information on default values for the OS build process within Opsware SAS and contains the following topics:

- Overview of Default Values for the OS Build Process
- Custom Attributes for Sun Solaris
- Custom Attributes for Linux
- Custom Attribute for Microsoft Windows
- Adding Custom Attributes to an OS Definition

Overview of Default Values for the OS Build Process

In addition to the customization provided by using build customization scripts, each build script uses custom attributes.

The Opsware Command Center provides a data management function by allowing users to set custom attributes for servers. These custom attributes include setting miscellaneous parameters and named data values. Users can write scripts that use these parameters and data values when performing a variety of functions, including network and server configuration, notifications, and CRON script configuration.

See “Custom Attributes Set for the Environment” on page 287 in Chapter 10 for information about custom attributes.

For OS provisioning, Opsware SAS uses custom attributes to pass specific information to each build script to configure aspects of the installation process.

You can edit an OS definition to override the default values used by the build process. You override these default values by setting custom attributes for the OS definition.

See “Adding Custom Attributes to an OS Definition” on page 141 in this chapter for information about the steps to set custom attributes for an OS definition.

Custom Attributes for Sun Solaris

The build script for Solaris OS provisioning uses a number of custom attributes. Several of these custom attributes correlate with an equivalent setting that would be defined normally by a Solaris `sysidcfg` file.

You cannot modify the `sysidcfg` file that the OS Provisioning feature uses. However, you can override specific values specified in the default `sysidcfg` file. You can set custom attributes for a Solaris OS definition in the Opsware Command Center.

The custom attributes correspond to the equivalent keywords in the `sysidcfg` file. See Table 5-5.

Table 5-5: Sun Solaris Custom Attributes

KEYWORD	DESCRIPTION
`root_password`	Sets the encrypted value for the password on an installation client. One way to obtain an encrypted value is by using `/etc/shadow`. If a value is not set, the system will not have a root password.
`timezone`	Sets the time zone in which to configure the installation client (sets `TZ` in `/etc/default/init`). The directories and files in the directory `/usr/share/lib/zoneinfo` provide the valid time zone values. By default, the timezone value is UTC. For example, the time zone value for Pacific Standard Time in the United States is `US/Pacific`. You can also specify any valid Olson time zone.

Table 5-5: Sun Solaris Custom Attributes

KEYWORD	DESCRIPTION
`system_locale`	Sets the language in which to configure the installation client (sets `LANG` in `/etc/default/init`). Valid locale values are installed in `/usr/lib/locale`. If you set this attribute, you should also use the `locale` keyword in the operating system profile so that the appropriate locale is installed. By default, the value for this keyword is `system_local=C`.
`required_patches`	This keyword is reserved by the Solaris build script. Using it might cause the installation process to fail. To specify required patches, include them with the OS definition in a template. See “Opsware Patch Management” on page 323 in Chapter 11 for more information about how patch management works in Opsware SAS.
`nfsv4_domain`	Sets the system’s default NFS version 4 domain name. If this value is not set, the OS Provisioning feature suppresses the prompt to confirm the NFS version 4 domain name when the server starts the first time.

Custom Attributes for Linux

You can use custom attributes to specify additional arguments to the kernel under which the installation is running. By specifying these arguments, you can accomplish tasks such as pinning interfaces. The OS Provisioning feature appends the contents of the custom attribute to the kernel arguments for the kernel that is installing the OS.

Set a custom attribute for the OS definition (edit the OS definition and click the Custom Attributes tab). The custom attribute must have the name `kernel_arguments`.

The kernel arguments are separated by spaces (like they are when you type them after the boot prompt for the CD-ROM or DVD). For example:

```
name=value jones=barbi
```

To have the kernel arguments persist after the base OS is installed, you must set them in the uploaded configuration file. Setting kernel arguments by using custom attributes only allows you to create a completely automated installation (as if you were installing the OS from CD-ROM or DVD).

Custom Attribute for Microsoft Windows

For a Windows OS definition, you can set a value for the `timeout` custom attribute. Setting this value controls the timeout value after an error.

Set this value to the amount of time (in minutes) it takes Windows setup to complete.

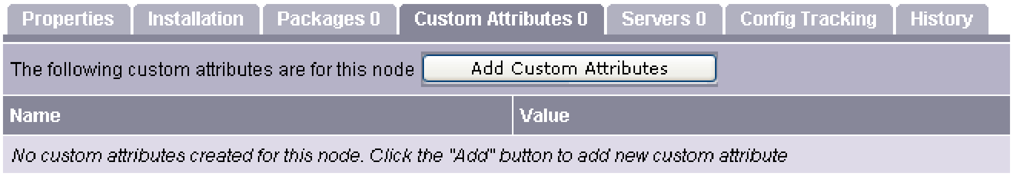
If Windows setup does not complete in the specified amount of time, the OS installation will fail with a timeout error. By default, this value is set to 60 minutes.

Adding Custom Attributes to an OS Definition

Perform the following steps to add custom attributes to an OS definition:

1. From the navigation panel, click Software ➤ Operating Systems. The Operating Systems page appears.
2. Click the display name of the OS that you want to edit. The Edit Operating System page appears.
3. Click the Custom Attributes tab. The list of custom attributes specified for the OS definition appears, as Figure 5-10 shows.

Figure 5-10: Custom Attributes Tab for an OS Definition in the Opsware Command Center



The following custom attributes are for this node

Name	Value
No custom attributes created for this node. Click the "Add" button to add new custom attribute	

If the OS definition contains custom attributes, the Edit Custom Attributes button appears in the page. Click the Edit Custom Attributes button to add new attributes and edit existing ones.

4. Click the Add Custom Attribute button. A page appears in which you can enter the names and values for custom attributes.

5. Enter a name and a value for the custom attribute.
6. Click the Save button. The list of custom attributes set for the OS definition reappears. The new custom attribute is added to the list.

Overview of Including OS Definitions in Templates

In Opsware SAS, you can create templates to automate building complete server baselines.

By using Opsware templates, system administrators can define and provision servers with standard configurations, sometimes called *server baselines*. For example, system administrators can define a Windows baseline for databases, a Windows baseline for Web and application servers, and a different Windows baseline for messaging servers. Each baseline can include a different variant of the following items:

- A base operating system
- The latest operating system patches
- System utilities such as SSH or PC Anywhere
- Security tools such as TripWire or anti-virus software
- Widely shared system software such as the latest Java Virtual Machine

Using templates, which are pre-packaged collections of installable software, users can provision an entire software stack, including the base operating system, the latest set of operating system patches, system utilities such as SSH and the latest JVMs, middleware including databases, Web servers, and application servers, and so on, up to the custom business applications that the server ultimately runs.

See “Templates and Folders” on page 291 in Chapter 10 for information about how to create and edit templates to include OS definitions.

Hardware Support in OS Provisioning

This section provides information on hardware support in OS provisioning within Opsware SAS and contains the following topics:

- Overview of Hardware Support in OS Provisioning
- Overview of PXE Images for Windows and Linux

- Overview of Windows and Linux Boot Images
- About NIC Support in Windows Boot Images
- Adding NIC Support to a Windows Boot Image
- Sample Mapfile
- Sample Mapfile for an Intel 8255x-based PCI Ethernet Adapter
- Prerequisites for Creating Windows Boot Images
- Creating a Windows Boot Image
- Updating the PXE Image for Windows
- Adding Hardware Support to a Linux Build Image
- Creating a Linux Boot Image

Overview of Hardware Support in OS Provisioning

The OS Provisioning feature ships with support for a broad range of hardware platforms out of the box. Additionally, customers can add support to the OS Provisioning feature for hardware models not initially supported.

Preparing the OS Provisioning feature to provision new hardware is straightforward. The process involves packaging and uploading system utilities that the server manufacturer provided into Opsware SAS.

At a minimum, the boot processes for Windows and Linux (Opsware Boot Floppies or CDs and the PXE boot system) must be updated to support the new hardware.

Additionally, the Linux build images themselves might need to be updated to support the new hardware.

See “Adding NIC Support to a Windows Boot Image” on page 146 in this chapter for more information.

See “Adding Hardware Support to a Linux Build Image” on page 151 in this chapter for more information.

Overview of PXE Images for Windows and Linux

The OS Provisioning feature supports booting new x86-processor-based servers with the Preboot Execution Environment protocol (PXE).

When Opsware SAS was installed with the Opsware Installer, a default boot image was added to the PXE system for Windows and for Linux so that new servers can be booted for the first time over the network. The boot image is used by Opsware SAS as the second stage PXE image for PXE network bootstrap programs such as PXELinux.

For Linux, Opsware SAS includes a boot image that contains the `bootnet.img` CD for Red Hat Linux AS 3.0. The image has changes to the `syslinux.cfg` and `boot.msg` files; however, the kernel and `initrd.img` are identical to the files on the Linux OS media.

The default boot images include common NIC drivers for many hardware makes and models. Opsware SAS uses these NIC drivers to boot new x86-processor-based servers for the first time.

The Linux PXE image and Linux Boot CD contain the same NIC drivers included on the Red Hat Linux AS 3.0 installation CD-ROM or DVD.

Table 5-6 shows the Windows boot image, which includes the following set of common NIC drivers.

Table 5-6: NIC Drivers Included with the Windows Boot Image

DRIVER NAME	DESCRIPTION
B57	Broadcom NetXtreme Gigabit Ethernet NDIS2 Driver v5.20 (021025)
DC21X4	Digital 2104x/2114x 10/100 mbps Ethernet Controller v3.00
E1000	Intel 8254X Based Adapter (pro/1000 gigabit) v1.28 040302
E100B	Intel(R) PRO PCI Driver v4.35 042902
EL59X	3Com DOS NDIS driver for 3C59X Family Adapters v1.2f
EL90X	3Com Etherlink PCI DOS NDIS driver v5.2.2
ELNK3	3Com DOS EtherLink 10 ISA (3C509b) Network Driver v3.1
ELPC3	3Com Megahertz Ethernet PC Card 589E DOS Netw. Driver v1.9.002
ELPC575	3Com Megahertz 10/100 LAN CardBus PC Card DOS NDIS driver v3.4b
FA31X	Netgear FA310TX Fast Ethernet PCI Adapter
FETND	VIA Rhine Family Fast Ethernet Adapter Driver v4.05
N100	Compaq Fast Ethernet and Gigabit NDIS 2 NIC Drivers 7.0a (25Jan02)

Table 5-6: NIC Drivers Included with the Windows Boot Image

DRIVER NAME	DESCRIPTION
NE2000	Microsoft NE2000 NDIS Driver
NETFLX3	Compaq NetFlex-3 DOS NDIS 2.02 driver
PCNTND	AMD PCNet Family Ethernet Adapter NDIS v2.0.1 MAC Driver v3.12
RTSND	Realtek RTL8139/810X Family PCI Fast Ethernet v3.23 07/28/99
SMC9432	SMC EtherPower II 10/100 (9432TX) v1.02c (970605)

If the NIC drivers that you need for your environment are not included in the default set, you must perform the following tasks:

- Add them to the boot image for Windows, Linux, or both.
- Update the Windows or Linux boot image in the PXE system with the new boot images.

Overview of Windows and Linux Boot Images

For environments with servers that do not support network boot technology, Opsware SAS supports floppy- or CD-based booting.

You can create a Windows boot floppy from the default boot image for Windows. Opsware SAS includes the Opsware Build Image Administrator, a tool for creating a boot floppy for Windows.

For Linux, you can download the boot image for Linux from the Opsware Command Center. Search for the package name `bootfloppy` and package type `Unknown` in the Packages section of the Opsware Command Center. Download and create a Linux Boot CD from this image.

See “Creating a Linux Boot Image” on page 151 in this chapter for more information.

About NIC Support in Windows Boot Images

Opsware SAS includes a default set of common NIC drivers for many hardware makes and models. If the NIC drivers you need for your environment are not included in the default set, you must add them to the boot image for Windows.

The Opsware Build Image Administrator has the ability to dynamically detect your server's PCI network adapter. It does this by scanning the PCI bus for PCI information and comparing the information against each entry in a driver catalog until it finds a match. The driver catalog is constructed each time you create a boot image with the Opsware Build Image Administrator.

Each properly formatted cabinet file in the directory `\content\drivers\ndis` under the Opsware Build Image Administrator directory is included as an entry in the driver catalog.

Adding NIC Support to a Windows Boot Image

Before you perform this procedure, you must obtain the appropriate NDIS2 network drivers and `protocol.ini` file for the card from the manufacturer of the card.

Perform the following steps to add NIC support to a Windows boot image:

1. Create a temporary working directory for accumulating files that becomes part of the cabinet file.
2. Place NIC drivers and the `protocol.ini` files in the temporary directory.
3. Create a text file called `ndis.pci` in the temporary working directory.
4. Using a PCI bus scanner, determine the PCI vendor ID and device ID of the NIC card.

   For example, the 8255x-based PCI Ethernet Adapter from Intel has vendor ID 8086 and device ID 1229.
5. Using the vendor ID and device ID you obtained for the NIC, construct the mapfile `ndis.pci`.

   In the mapfile, lines that begin with a semicolon (;) are treated as comments and ignored.

   The sample mapfile in this chapter contains comment lines so that you can use it as a header for your mapfile.
6. Create a file named `ndis.txt` in the temporary directory that contains the following single line of text:

   ```
   [basename of cabinet file] "[Driver description string]"
   ```

   The information in this file is used to make up a selection list if the PCI adapter cannot be automatically detected.

   Example `ndis.txt` file for the `E100B.CAB`:

```
E100B   “Intel(R) PRO PCI Driver v4.35 042902”
```

7 Create the cabinet file by using cabarc and copy the cabinet file to the directory `.\content\drivers\ndis` under the Opsware Build Image Administrator directory. (Cabarc is a Microsoft utility that creates, extracts, and lists the contents of cabinet files.)

```
E:\temp\temp_cab>cabarc N e100b.cab *
Microsoft (R) Cabinet Tool - Version 5.2.3718.0
Copyright (c) Microsoft Corporation. All rights reserved.
Creating new cabinet 'e100b.cab' with compression 'MSZIP':
-- adding e100b.dos
-- adding e100b.ini
-- adding ndis.pci
-- adding ndis.txt
Completed successfully
```

Sample Mapfile

Modify the contents of this sample mapfile. This sample mapfile contains comment lines so that you can use it as a header in the mapfile that you create.

```
; Mapfile for PCISCAN "PCI PnP for DOS"
;
; Syntax:
;    ret="string_to_return"
;    ven=<vendorID> ["Vendor description"]
;    dev=<deviceID> ["Device description"]
;
; Example:
;    ret="aspi8dos.sys"
;    ven= 9004 "Adaptec"
;    dev= 7078 "Adaptec AIC-7870 PCI SCSI Controller"
;       7178 "Adaptec AHA-294X/AIC-78XX PCI SCSI Controller"
;       7278 "SCSI Channel on Adaptec AHA-3940/3940W PCI SCSI
;       Controller"
;       7478 "Adaptec AHA-2944 PCI SCSI Controller"
```

```
    ;       7578 "SCSI Channel on Adaptec AHA-3944 PCI SCSI
    ;       Controller"
    ;       7678 "Adaptec AIC-7870 based PCI SCSI Controller"
```

Sample Mapfile for an Intel 8255x-based PCI Ethernet Adapter

```
ret="E100B"
ven=8086 "Intel"
dev=1002 "PRO 100 Mobile Adapters"
    1031 "PRO/100 VE Network Connection"
    1032 "PRO/100 VE Network Connection"
    1035 "PRO/100 VM Network Connection"
    1036 "82562EH based Phoneline Network Connection"
    1038 "PRO/100 VM Adapter"
    1039 "PRO/100 VE Network Connection"
    103b "PRO/100 VM Network Connection"
    103c "PRO/100 VM Network Connection"
    103d "PRO/100 VE Network Connection"
    103e "PRO/100 VM Network Connection"
    1059 "PRO 100 Mobile Adapters"
    1229 "8255x-based PCI Ethernet Adapter (10/100)"
    2449 "PRO/100 VE Desktop Adapter"
    2459 "82562 based Fast Ethernet Connection"
    245d "82562 based Fast Ethernet Connection"
```

Prerequisites for Creating Windows Boot Images

The Opsware Build Image Administrator is used to create a Windows Boot Image that installs the OS Build Agent on servers. The Opsware Build Image Administrator is packaged with MSI.

You must meet the following requirements to use the Opsware Build Image Administrator:

- The machine on which the Opsware Build Image Administrator is installed must have a Python interpreter installed. You can obtain a Python interpreter from ActiveState.

- Opsware SAS includes a default set of common NIC drivers for many hardware makes and models. If the NIC drivers that you need for your environment are not included in the default set, you must add them to the floppy image.

  See “Adding NIC Support to a Windows Boot Image” on page 146 in this chapter for more information.

Creating a Windows Boot Image

Perform the following steps to create a Windows boot image:

1. Download the MSI package that contains the Opsware Build Image Administrator by downloading the file `opswbia-<version>-0.msi` from the Opsware Command Center.

   Where `<version>` is the latest version of the Opsware Build Image Administrator tool for the release of Opsware SAS installed at your facility. Only one version of the Opsware Build Image Administrator tool is available on the Software Repository.

   See “Downloading a Package” on page 224 in Chapter 7 for more information.

2. Install the MSI package that contains the Opsware Build Image Administrator tool on a Windows server that has a Python 1.5.2 interpreter.

   By default, the Opsware Build Image Administrator is installed in the following directory:

   ```
   %SystemDrive%\Program Files\OPSWBIA
   ```

3. Change directories to the Opsware Build Image Administrator installation directory:

   ```
   \Program Files\OPSWBIA >
   ```

4. Insert a disk into drive A.

5. Run the python script `mkimage.pyc`.

   ```
   \Program Files\OPSWBIA > python mkimage.pyc <options>
   ```

   If you do not enter any options, the Opsware Build Image Administrator creates a PXE build image file `dosopsw.1` in the current working directory. Enter the `-w` option to write the file `dosopsw.1` to a disk.

Details: Options for the Opsware Build Image Administrator

You can use the options that Table 5-7 shows when you run the Opsware Build Image Administrator from the command line.

Table 5-7: Opsware Build Image Administrator Command Line Options

OPTION	DESCRIPTION
`-a` <*drive*>	Writes the boot image to this drive (Default drive: `A`)
`-c`	Makes an el-torito bootable CD image in addition to the boot image
`-d`	Enables debugging of the OS Build Agent in the generated image
`-f`	Formats the disk first when writing to a disk
`-h` <*host*>	Specifies the hostname for the Agent Gateway (required option)
`-i` <*file*>	Specifies the filename for the generated boot image (Default filename: `dosopsw.1`)
`-n` <*directory*>	Specifies the directory where NDIS driver packages are located (Default directory: `./content/ndis`)
`-o` <*OS*>	Sets the OS for the boot image (Default OS: `dos622`)
`-p` <*port*>	Sets the port for the OS Build Agent to use to contact the Agent Gateway (Default port: `8017`)
`-t`	Performs a test image generation and does not execute any commands
`-w`	Writes the generated image to a disk in the drive specified by the option `-a`

Updating the PXE Image for Windows

When Opsware SAS was installed with the Opsware Installer, an image was added to the PXE system by default. You only need to update the PXE image when you have added support for additional NIC drivers to the image.

See “Adding NIC Support to a Windows Boot Image” on page 146 in this chapter for more information.

After adding NIC support to the boot image, install the boot image by using `scp` to copy the image file into the `/opt/OPSWboot/tftpboot` directory on the Opsware Build Server.

Adding Hardware Support to a Linux Build Image

You can modify the OS Provisioning feature to add new hardware support to a Linux build image. To provision servers with a Linux OS, Opsware SAS uses two types of Linux build images:

- A Linux Boot Image – Opsware SAS uses a modified version of Red Hat Linux AS 3.0 as a bootstrap image. The Linux Boot Image is loaded on servers when they are booted up for the first time by using the Linux Boot CD or by using PXE. The server appears in the Server Pool list and is ready to be provisioned with an OS.
- A Linux Build Image that installs the target OS – Opsware SAS uses this type of Linux Build Image to install the target Linux OS on servers.

To add new hardware support to a Linux Build Image, you must recompile the kernel and modules, and insert the modules into the `initrd.img` file and replace the kernel if it changed.

The Linux Build Images are located on the OS Build Manager host in the following directories:

```
/cust/buildscripts/linux/bi-<version>
```

Where `<version>` is the version of Linux.

When you modify the Linux Boot Image, include the following options in the kernel:

```
CONFIG_PACKET=y
CONFIG_FILTER=y
```

Setting these options is required if you want to retrieve the Build Manager parameters from DHCP. The existing Linux Boot Image is compiled with these options.

See the Red Hat Linux or SUSE Linux documentation for information about how to add hardware support.

Creating a Linux Boot Image

Opsware SAS includes a command line utility, OPSWlinuxbootiso, that you can use to create a Linux Boot Image on CD. Running the `mkcdrom.sh` script of OPSWlinuxbootiso creates an ISO file that you can write to a CD.

1. In the Opsware Command Center, search for the package name `OPSWlinuxbootiso*` and operating system Red Hat Enterprise Linux AS 3.0. See “Searching for Packages” on page 208 in Chapter 7 for more information.

2. Download the package to a server or desktop running Linux. See “Downloading a Package” on page 224 in Chapter 7 for more information.

3. On the server or desktop where you downloaded the OPSWlinuxbootiso utility, verify that version 1.10-4 of the mkisofs utility is installed.

4. Change to the following directory:

   ```
   cd /opt/OPSWlinuxbootiso
   ```

5. Run the `mkcdrom.sh` script:

   ```
   ./mkcdrom.sh <file-name.iso>
   ```

6. At the prompts, enter the following information:

   - The IP address or hostname of the core server running the Agent Gateway (default hostname: `buildmgr`)
   - The port on the Agent Gateway that is forwarded [default: 8017]
   - The IP address or hostname of the Boot Server (default hostname: `buildmgr`)
   - The path to the media for the OS Build Agent (default path: `/opt/OPSWboot/kickstart`)
   - The network interface from which to run Linux Kickstart

Example: Usage of the OPSWlinuxbootiso Utility

```
sin: cd /opt/OPSWlinuxbootiso
sin: ./mkcdrom.sh /tmp/boot.iso
Please enter IP or hostname of Agent-Side Gateway [buildmgr]:
Please enter the port on the Agent-Side Gateway that is
forwarded [8017]:
Please enter IP or hostname of Boot Server[buildmgr]:
Please enter path to bootagent media[/opt/OPSWboot/kickstart]:
Please enter which network interface you would like to kickstart
from
(e.g. eth0) just press enter to choose at runtime:
buildmgr
8017
buildmgr
/opt/OPSWboot/kickstart
*********************************************
* Rewritting isolinux.cfg                   *
*********************************************
*********************************************
* Building iso... /tmp/fooboot.iso
```

```
*********************************************
INFO:   UTF-8 character encoding detected by locale settings.
        Assuming UTF-8 encoded filenames on source filesystem,
        use -input-charset to override.
Size of boot image is 4 sectors -> No emulation
Total translation table size: 2048
Total rockridge attributes bytes: 0
Total directory bytes: 2048
Path table size(bytes): 26
Max brk space used 0
1858 extents written (3 MB)
sin:/opt/OPSWlinuxbootiso>
```

Chapter 6: OS Installation Integration

IN THIS CHAPTER

This chapter discusses how to integrate Opsware SAS with operating system installation technologies. This chapter discusses the following topics:

- OS Installation Technologies
- OS Installation Integration
- Integration High-Level Steps
- Integration with Red Hat Kickstart
- Integration with Solaris JumpStart
- Integration with Windows OS Installation Technologies
- Example: Integration with Windows NT and Symantec Ghost
- Integration with Network Installation Management and AIX
- Integration with Ignite-UX and HP-UX

Opsware SAS includes the OS Provisioning feature, which allows you to install the following versions of Sun Solaris, Linux, and Microsoft Windows operating systems:

- Windows NT 4.0, 2000, and 2003
- Red Hat Linux 7.1, 7.2, 7.3, 8.0, 2.1 AS/ES/WS, 3 AS/ES/WS, and 4 AS/ES/WS
- SUSE Linux Standard Server 8.0, SUSE Linux Enterprise Server 8.0, and SUSE Linux Enterprise Server 9.0
- Sun Solaris 7, 8, 9, and 10

See “OS Provisioning Setup” on page 93 in Chapter 5 for more information about the instructions to set up Opsware SAS to provision servers with Solaris, Linux, and Windows.

Alternatively, you can integrate Opsware SAS with an OS installation technology that is already functioning in your operational environment. Using a third-party installation technology enables installing an OS by using vendor utilities and automatically installing the Opsware Agent, which registers servers with the Model Repository.

The OS Provisioning feature does not provision HP-UX or AIX operating systems. Follow the procedures in this appendix to integrate Opsware SAS with Network Installation Management (NIM) to provision AIX and Ignite-UX to provision HP-UX.

OS Installation Technologies

Operating system (OS) vendors provide automation technology for installing their operating systems. OS installation technologies follow this general process:

1. Boot the server from boot media.
2. Partition and format the target disks.
3. Install the OS onto the target disks.
4. Reboot the server from the newly installed OS.

For example, Solaris JumpStart follows this process:

1. Boot the server from the network.
2. Partition and format the server's disks.
3. Install the OS, optionally installing additional patches and packages.
4. Reboot the server from the newly installed OS.

OS installation technologies provide a way to invoke customer-supplied code at the end of the OS installation process. After the operating systems are installed, users can run scripts or programs to customize servers. Opsware SAS uses this integration point to automatically install the Opsware Agent and register the servers with the Model Repository.

OS Installation Integration

This section provides information on OS installation integration and contains the following topics:

- Overview of OS Installation Integration
- Modeling Operating Systems
- How Opsware SAS Manages Servers

Overview of OS Installation Integration

Opsware SAS integrates with OS installation technologies, including third-party and vendor-provided OS bootstrapping technologies. These OS installation technologies give you the ability to set up unattended OS installations. You boot a system and the software installs automatically.

Integrating with these technologies provides a uniform method for OS installation because Opsware SAS conforms the installed OS to the data model in the Model Repository of what OS software should be installed.

Servers conform to the model because Opsware SAS installs patches, Service Packs, or Hotfixes, installs other software (such as SSH), removes software, turns processes on and off (such as turning off the FTP server), and updates configurations.

Modeling Operating Systems

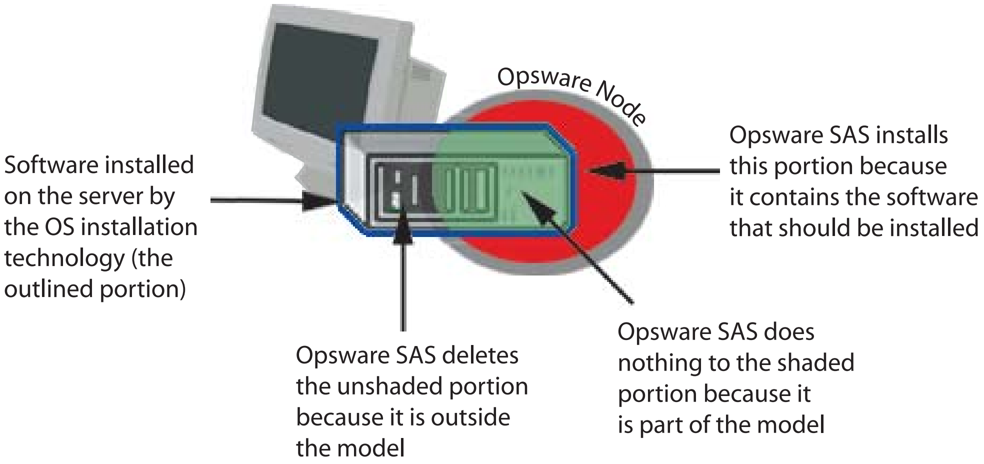
To manage servers' operating systems by using Opsware SAS, you model the operating systems in the Opsware Command Center. An OS model is represented as a template that specifies a set of nodes assigned to servers when the template is applied to the servers. The Node assignments enable Opsware SAS to conform the OS on the servers to the model of what should be installed on servers.

When you model an OS:

- Patches, Service Packs, and software that are specified in the model are installed after the server's OS is installed. Modeling an OS ensures that all newly provisioned servers have required patches, security fixes, and utility software installed automatically.

- Software that is not part of the model can optionally be removed.

Figure 6-1: How the Opsware Model Affects Software Installation


Opsware Node
Software installed on the server by the OS installation technology (the outlined portion)
Opsware SAS installs this portion because it contains the software that should be installed
Opsware SAS deletes the unshaded portion because it is outside the model
Opsware SAS does nothing to the shaded portion because it is part of the model

When you do not model an OS in Opsware SAS:

- The Opsware Agent can be automatically installed, and the server can be registered with the Model Repository.
- Opsware SAS removes only software that was previously installed by Opsware SAS and does not disrupt an OS that an OS installation technology installed.
- However, Opsware SAS cannot manage the OS software until a model of the OS is created and the server is associated with that model.

How Opsware SAS Manages Servers

Opsware SAS manages servers by automatically installing the Opsware Agent and registering the servers with the Model Repository.

After an OS is installed with an installation technology, a user can run a post-installation script to customize the server. In the script, the user can include logic to invoke the Opsware Agent Installer, so that the following actions are performed:

1. The Opsware Agent Installer installs an Opsware Agent on the server.
2. The Opsware Agent gathers information about the server (such as hardware attributes) and registers the server with the Model Repository.
3. Opsware SAS attaches the server to the appropriate hardware, facility, and customer nodes.

The server is associated with the default facility for the local instance of Opsware SAS.

If IP address ranges are specified for customers in Opsware Command Center, the server is associated with the customer through its IP address.

If the server's IP address does not fall within a specified IP address range, the server is associated with the default IP range group (the "Default" IP range group). The default group is associated with the "Not Assigned" customer.

4. Opsware SAS assigns the server to an OS Template, which designates sets of node assignments. This information enables Opsware SAS to conform the OS to a model of what should be.

   For example, all Windows 2000 servers can be attached to an OS Template that specifies that a given service pack should be applied to the servers.

   If an OS Template is not specified, Opsware SAS attaches the server to a generic Template that is empty (it does not contain software).

5. (Optional) Opsware SAS reconciles the server, which conforms the server with the model by installing patches (Service Packs and Hotfixes for Windows), installing software (such as, the latest version of SSH), removing software, turning processes on and off (such as turning off the FTP server), and updating configurations.

Integration High-Level Steps

This section provides information on how to integrate Opsware SAS into a network environment and contains the following topics:

- Integrating Opsware SAS
- Opsware Agent Installer Commands and Options
- Opsware Agent Installer Options
- Examples: Opsware Agent Installer Command and Options

Integrating Opsware SAS

Regardless of the OS installation technology used in the managed environment, you integrate Opsware SAS in this general way:

1. Make the Opsware Agent Installer binary available to the server, through NFS mount, by copying the installer to a local disk, by using wget, or through another method.

The Opsware Agent Installer binary must be available to the post-installation scripts when they run.

2. Include logic in a post-installation script or file (Windows) for the OS installation technology to assimilate the server by running the Opsware Agent Installer with the appropriate options.

   - Unix: Write out a script that runs on reboot, installs the Opsware Agent on the server, and then removes itself.
   - Windows 2000: Run commands in a post-installation script by using the `[GuiRunOnce]` section in unattended installation files or in the file sysprep.inf.
   - Windows NT: Insert an entry in the Registry to call a batch file that runs once at startup and specifies the Opsware Agent Installer options in a post-installation script.

The post-installation script or commands must arrange for the server to be assimilated the first time it reboots after OS installation. Opsware SAS cannot assimilate a server until it reboots after OS installation. Before the reboot, the server is not running the final OS. Therefore, it is not appropriate to register the server with the Model Repository.

3. If you plan to manage the server's OS by using Opsware SAS (the `--template` and `--reconcile` options are specified with the Opsware Agent Installer), model the OS in Opsware Command Center. To model the OS in the Opsware Command Center, create Nodes and Templates for the OS and upload the OS packages to the Software Repository.

   See "Software Provisioning Setup" on page 247 in Chapter 10 for more information about how to model an operating system in the Opsware Command Center.

   See "Uploading a Package" on page 211 in Chapter 7 for more information about how to upload packages to the Package Repository.

Opsware Agent Installer Commands and Options

In the post-installation script or file, specify the correct Opsware Agent Installer for the operating system and the appropriate options for the installation environment.

Unix Executable

```
opsware-agent-<version>-<system_name>-<system_version>
```

Windows Executable

```
opsware-agent-<version>-<system_name>-<system_version>.exe
```

Opsware Agent Installer Options

Table 6-1: Agent Installer Options

OPTION	DESCRIPTION

`--clean`
`(-c)`
	Removes any machine-specific identifying material from the server. Specifically, removes the machine ID file (MID), and all machine-specific cryptographic material. Use this option when a server is deactivated and deleted from the Opsware Command Center and needs to be returned to service at a later time.

`-f`	Forces Opsware Agent installation and removes the target installation directory if it exists. REQUIREMENT: When using the `-f` option, you must run the Opsware Agent Installer as root on Unix operating systems and as the administrator on Windows operating systems.
`--logfile`	Specifies the path to the Opsware Agent Installer log file. By default, the current directory is set as the path. By default, the log file has the following filename: `opsware-agent-installer-<`*date*`>.log`
`--loglevel <`*level*`>`	Sets the log level for log messages. With this option, specify one of the following levels: `error`, `warn`, `info`, `trace`, or `none`. The level `error` logs the least detail. The level `trace` logs all messages. By default, the log level is set to the log level `info`.
`-o`	Logs all output to `stdout` instead of a log file. This option is invoked automatically if the default log file or the log file passed with the `--logfile` option cannot be created, for example, when running the Opsware Agent Installer from non-writeable media, such as a DVD.

Table 6-1: Agent Installer Options

OPTION	DESCRIPTION
`--reconcile` *<type>*	Reconciles the server against any nodes assigned to the server. The *<type>* can be `full` or `addonly`. `full` – All nodes in a category are selected and reconcile removes software that Opsware SAS did not install. `addonly` – Software installed outside of Opsware SAS is not removed. WARNING: When assimilating a server that is already functioning in the operational environment, use caution when specifying the option `--reconcile`. If you specify this option, you might inadvertently uninstall software from the server.
`--rpmbin` *<path>*	Specifies the path to the RPM binary to use for RPM operations. Use this option, when RPM is already installed on the server, to point the Opsware Agent at the RPM binary. Use the `--withrpm` option to install RPM if a usable instance of RPM is *not* already installed. NOTE: It is unnecessary to use this option with the `--withrpm` option.
`-s`	Starts the Opsware Agent after installing it. By default, the Opsware Agent Installer does not start the Opsware Agent.
`--template` *<ID>*	Assigns the nodes contained in the template to the server. `<ID>` can be an ID or a full name of a template. If this option is specified with the `--reconcile` option, Opsware SAS assigns the nodes in the template to the server before reconciling the server. WARNING: When assimilating a server that is already functioning in the operational environment, use caution when you specify the option `--template`. If you specify this option, you might inadvertently uninstall software from the server.

Table 6-1: Agent Installer Options

OPTION	DESCRIPTION
`--withmsi`	Installs MSI 2.0 along with the Opsware Agent. If MSI 2.0 is already installed, this option has no effect. Works with Windows NT 4.0 Service Pack 6a, Windows 2000, and Windows 2003.
`--withwmi`	Installs WMI 1.5 along with the Opsware Agent. If WMI 1.5 is already installed, this option has no effect. Works with Windows NT 4.0 Service Pack 6a.
`--withrpm`	Installs the RPM handler with the Opsware Agent. By default, an Opsware Agent is not installed with this option. Opsware Inc. recommends that you always include the `--withrpm` option when you install Opsware Agents on Solaris servers. NOTE: Use the `--withrpm` option only with the Opsware Agent Installers for these operating systems: Solaris 5.6, 5.7, 5.8, and 5.9, and AIX 4.3 and AIX 5.1. On Solaris, RPM 3.0.6 is installed in the directory `/opt/OPSWrpm` and the RPM database is installed in the directory `/var/opt/OPSWrpm/lib/rpm`. On AIX, RPM 3.0.5 is installed in the directory `/opt/freeware` and the RPM database is installed in the directory `/var/opt/freeware/lib/rpm`.
`--workdir` <*path*>	Specifies the path to the Opsware Agent Installer temporary working directory. Use this option if the default working directory causes problems with installation.

Table 6-1: Agent Installer Options

OPTION	DESCRIPTION
`--reboot`	During Opsware Agent Installation on a Windows server, the Agent Installer copies the ogshcap.dll file to the following location: `%SystemRoot%\system32\ogshcap.dll` If the file is open or is in use, the Agent Installer is unable to copy the ogshcap.dll file. The Agent Installer then informs the user whether to restart the machine and copies the file after restart. You can specify the `--reboot` Installer option in the Opsware Command Line to initiate the reboot at the end of the Agent installation.
`--resetconf(-r)`	Resets Opsware Agent configuration file to default the settings.
`--no_anonymous_ssl (-A)`	Disables anonymous SSL. This option applies to dormant Opsware Agents only. This option configures the Opsware Agent so that browsers cannot connect without a valid certificate.

Table 6-1: Agent Installer Options

OPTION	DESCRIPTION
`--settime (-t)`	Synchronizes the time on the server on which the Opsware Agent is installed with that of the Opsware core. NOTE: If the server on which the Opsware Agent is being installed is significantly ahead of the clock on the Opsware core, then the clock on the managed server is set back in time. Since this can cause problems, do not use the --settime option unless you are sure that this scenario is not a problem in your environment. If a managed server's clock is significantly behind of the clock on the Opsware core, the Opsware Agent installation might fail. To install an Opsware Agent successfully, use the `--settime` option or manually set the time and date on the managed server before retrying the Opsware Agent installation.

Examples: Opsware Agent Installer Command and Options

Enter the following command and options to install the Opsware Agent for Solaris 5.7 in the default directories and log results of the installation in the log file:

```
% opsware-agent-1.0.0-solaris-5.7 --logfile opsware-agent-
installer-[current_date].log --loglevel info
```

Enter the following command and options to install the Opsware Agent for Windows NT 4.0 in the default directories and log results of the installation in the log file:

```
% opsware-agent-1.0.0-win32-4.0.exe --logfile opsware-agent-
installer-[current_date].log --loglevel info
```

Integration with Red Hat Kickstart

Red Hat Kickstart uses a configuration file that contains a number of distinct sections. The section `%post` contains a set of commands to run after the OS installation is complete.

Perform the following steps:

1. Copy the Opsware Agent Installer to local disk storage, for example `/var/tmp,` on the server on which the Opsware Agent is being installed.

Copy the Opsware Agent Installer to a directory that will not be empty when the server reboots. The operating system might empty the contents of the `/tmp` and `/var/tmp` directories when the server reboots.

2. Create an init script that includes the following logic to invoke the Opsware Agent Installer on reboot, and then remove itself:

```
cp /<volume>/<agent_installer> <installer_local_path>
cat > /etc/rc.d/rc3.d/S99zAgentInstaller << EOF
#!/bin/sh
<installer_local_path> <agent_installer_options>
if [ $? -eq 0 ]; then

   rm -f /etc/rc.d/rc3.d/S99zAgentInstaller

   rm -f <installer_local_path>

fi
EOF
```

The script `S99zAgentInstaller` removes itself and the Opsware Agent Installer binary when the Opsware Agent Installer returns zero. If the installation returns an error, the script `S99zAgentInstaller` will not remove itself from the server and will attempt installation on the next reboot. Alternatively, you can rerun the init script manually (you must be root).

Example File: init Script for Kickstart

The following example assumes that the Opsware Agent Installer binary is available by using an NFS volume mounted at /sw.

```
cp /sw/opsware-agent-5.1.14-linux-7.2 /var/tmp/opsware-agent-
installer
cat > /etc/rc.d/rc3.d/S99zAgentInstaller << EOF
#!/bin/sh
```

```
/var/tmp/opsware-agent-installer --template 12340002 --settime
--reconcile full
if [ $? -eq 0 ]; then
   rm -f /etc/rc.d/rc3.d/S99zAgentInstaller
   rm -f /var/tmp/opsware-agent-installer
fi
EOF
```

Integration with Solaris JumpStart

Solaris Jumpstart uses a profile that is capable of running a post-installation script (also referred to as a finish script). The post-installation script contains a set of commands to run after the OS installation is complete.

When you integrate tOpsware SAS with Solaris Jumpstart, use a post-installation script to perform the following actions:

1. Copy the Opsware Agent Installer to local disk storage, for example `/var/tmp,` on the server on which the Opsware Agent is being installed.

Copy the Opsware Agent Installer to a directory that will not be empty when the server reboots. The operating system might empty the contents of the `/tmp` and `/var/tmp` directories when the server reboots.

2. Create an init script that invokes the Opsware Agent installer on reboot, and then remove itself.

Example File: Jumpstart Finish Script

The following example assumes that the Opsware Agent Installer binary is installed in the Jumpstart configuration directory.

For use in a post-installation script, Jumpstart automatically sets the variable `$SI_CONFIG_DIR` to refer to the Jumpstart configuration directory. See the *Solaris Advanced Installation Guide* for information.

```
#!/bin/sh
#
# finish script which adds agent installer during Jumpstart
#

AGENT=opsware-agent-5.1.35-solaris-5.8
AGENT_START_SCRIPT=/etc/rc3.d/S99zAgentInstaller
TEMPLATE_ID=12345

# copy agent installer to client's /var/tmp
# client's filesystem is mounted as /a during jumpstart
cp $SI_CONFIG_DIR/$AGENT /a/var/tmp/opsware-agent-installer
chmod 0755 /a/var/tmp/opsware-agent-installer

# setup a script to run the installer on reboot
touch /a/$AGENT_START_SCRIPT
chmod 711 /a/$AGENT_START_SCRIPT
chown root:sys /a/$AGENT_START_SCRIPT

cat >> /a/$AGENT_START_SCRIPT << EOF
#!/bin/sh
exec > /var/tmp/`basename $AGENT_START_SCRIPT`.log 2>&1
set –x
/var/tmp/opsware-agent-installer \
        --template $TEMPLATE_ID \
        --settime \
        --reconcile addonly \
        --decommission \
        --logfile /var/tmp/opsware-agent-installer.log

if [ \$? -eq 0 ]; then
  cp $AGENT_START_SCRIPT /var/tmp/
  rm -f $AGENT_START_SCRIPT
fi
EOF
```

Integration with Windows OS Installation Technologies

This section provides information on integrating with Windows OS installation technologies within Opsware SAS and contains the following topics:

- Windows OS Installation Integration Process
- Example: Integration with Windows 2000 and Symantec Ghost
- Running the Opsware Agent Installer by Using Sysprep
- Example File: Preparing a Windows 2000 System for Imaging
- Example Batch File: Running the Agent Installer for Windows 2000

Windows OS Installation Integration Process

Integrating Opsware SAS with Windows OS installation technologies follows this general process:

1. Install a Windows operating system (2000 or NT) on a server. Install the OS manually (by using a CD or from a network) or use a vendor OS installation technology, for example:

    - Imaging by using Symantec Ghost

      Symantec Ghost uses imaging technology to install operating systems onto servers. An image is a sector-by-sector copy of the entire contents of a disk. The image is installed in its entirety. You cannot use Symantec Ghost to selectively install parts of an image.

    - Imaging by using PowerQuest Drive Image and PowerQuest DeployCenter 5.0

      Deploy or upgrade Windows workstations or servers by remotely deploying an exact image of a hard disk.

    - Remote installation by using Microsoft Remote Installation Services (RIS)

      RIS is a program for installing Windows 2000, and applications and Service Packs. RIS is made up of individual services that are combined to enable the remote installation of Windows 2000.

    - Microsoft Systems Management Server (SMS)

      SMS deploys applications, software updates, and operating systems over simple or advanced enterprise networks.

2. Set up the Opsware Agent Installer to run the first time a system reboots after the OS installation. The Opsware Agent Installer assimilates a server by installing the Opsware Agent, reconciling the server (optional), and registering the server with the Model Repository.

- On Windows 2000, use Windows 2000 System Preparation Tool (Sysprep) to modify the Windows registry to run the Opsware Agent Installer. Sysprep is used to prepare Windows 2000 System Images as part of an automated deployment.
- On Windows NT, modify the Windows registry to run the Opsware Agent Installer once at startup after the Windows installation.

  Use the Windows registry entry to specify a batch file that lists the Opsware Agent Installer and associated options to run. You can specify the Opsware Agent Installer options to apply to a specific Windows server in a variety of ways; for example:

  - Maintain a file that maps server IP addresses or Ethernet MAC addresses to Opsware Agent Installer options and look up the server information in this file from the Opsware Agent Installer batch file.
  - If installing Windows from an image, prompt the user for the Opsware Agent Installer options when the server is running DOS before the Windows image is installed. Save the user input in an options file on the network. The options file will be specific to the Windows server being built. Read the option file from the Opsware Agent Installer batch file.

Example: Integration with Windows 2000 and Symantec Ghost

Integrating Opsware SAS with Windows 2000 and Symantec Ghost follows this two-phased process.

Phase 1: Create an image

1. Manually install Windows 2000 on a server and customize the installation as required.
2. Use the Microsoft utility sysprep to remove all machine-specific configuration, such as the Windows security identifier (SID), network configuration, and so forth.
3. Use Symantec Ghost to take an image of the server and save the image to a network share.

   See your Symantec Ghost documentation for information about this process.

Phase 2: Provision a server by using the image

1. Boot the server by using an MS-DOS boot diskette that contains Symantec Ghost (a DOS application).
2. Run Symantec Ghost and install the image created in Phase 1.

3 Reboot the server.

Windows runs a mini-setup wizard to configure the server.

4 Answer the prompts to the wizard. You can automate this process so that the answers to the wizard are pre-answered.

After the wizard finishes, the system reboots again and is ready for Opsware Agent installation.

5 Install an Opsware Agent on the server by running the Opsware Agent Installer and passing it the appropriate options.

See “Opsware Agent Installer Commands and Options” on page 160 in this chapter for information about a description of each option.

Automatically running the Opsware Agent Installer when using Symantec Ghost requires additional integration tasks. See “Running the Opsware Agent Installer by Using Sysprep” on page 171 in this chapter for information about.

Running the Opsware Agent Installer by Using Sysprep

A standard Windows 2000 unattended installation file has a [GuiRunOnce] section. During the installation process, this section automatically adds the section's entries into the computer's RunOnce registry subkey. When the computer's first user logs on, the computer executes any commands in the RunOnce registry entry, and then removes the commands from the registry.

Using Sysprep allows you to arrange for the Opsware Agent Installer to run automatically.

When using Sysprep to prepare a system for imaging, use the [GuiRunOnce] section in the file sysprep.inf to specify options for the Opsware Agent Installer when the server reboots after the setup wizard runs.

For example:

```
[GuiRunOnce]
"net use z: \\yourshare\software"
"z:opsware-agent-5.1.14-win32-5.0.exe --template 56780002
--settime --reconcile full"
```

The [`GuiRunOnce`] commands install the Opsware Agent each time the image is installed. However, the Opsware Agent Installer always runs with the same options. For example, if the commands include the `--template` and `--reconcile` options, you must create an image for each OS Template to which you plan to attach servers.

Use the [`GuiRunOnce`] section to run a batch file that specifies the Opsware Agent Installer options. Retrieving the options from a batch file allows you to specify the options when the image is installed (rather than when the image is created). For example, you could specify which `--template` and `--reconcile` options to use in a batch file.

For example:

```
    [GuiRunOnce]
    "net use z: \\yourshare\tools"
    "z:install-opsware-agent.cmd"
```

Example File: Preparing a Windows 2000 System for Imaging

The following example sysprep.inf file prepares the Windows 2000 system prior to imaging a disk. The file edits the Windows 2000 registry to call a batch file. The batch file is setup to run when the server reboots after image installation.

```
[unattended]
OemSkipEula = Yes

[Guiunattended]
OEMSkipRegional = 1
OEMSkipWelcome = 1
AdminPassword = PASSWORD
AutoLogon = Yes
AutoLogonCount = 2
TimeZone = 90

[UserData]
Computername = *
orgName = Opsware Inc.
ProductID = XXXXX-XXXXX-XXXXX-XXXXX-XXXXX <--replace with your
Windows 2000 CD product code
FullName = shadow

[LicenseFilePrintData]
AutoMode = PerServer
AutoUsers = 9999

[Networking]
InstallDefaultComponents = Yes

[Identification]
joinworkgroup = Embryo
```

```
[GuiRunOnce]
"net use z: \\imagestore.example.com\winimages"
"z:\tools\agent-install"
```

Example Batch File: Running the Agent Installer for Windows 2000

The following example batch file runs the Opsware Agent Installer and specifies the Opsware Agent Installer options. This batch file uses third-party freeware tools to perform DOS command line parsing and determine the server MAC address. The tool uses this value to locate the server-specific Opsware Agent Installer options.

This example batch file uses the following third-party tools:

- NBMAC (available from http://www.kostis.net/en)
- LMOD (available from http://home.mnet-online.de/horst.muc/)

```
@echo off
rem Find the appropriate arguments file
set prov_dir=z:
set params_dir=%prov_dir%\params
set tools_dir=%prov_drive%\tools

rem construct a unique temporary file name
set mac_file=%tmp%\%random%.bat
%tools_dir%\nbmac > %mac_file%

%tools_dir%\nbmac | lmod set mac_addr=[$1] > %mac_file%
call %mac_file%
del %mac_file%
find "rem mac_addr %mac_addr%" %params_dir%\*.arg

set foundfile=
for %%i in (%params_dir%\*.arg) do call findit.cmd %%i
if "%foundfile%"=="" goto notfound
echo Executing post-install commands from %foundfile%
copy %foundfile% %tmp%\opost.cmd
call %tmp%\opost.cmd

del %foundfile%
del %tmp%\opost.cmd
goto _end

:notfound
echo No post-install commands found for mac address %mac_addr%
goto _end
```

```
:_end
```

Example: Integration with Windows NT and Symantec Ghost

This section provides information on integrating Opsware SAS with Windows NT and Symantec Ghost and contains the following topics:

- Integrating with Windows NT and Symantec Ghost Process
- Example File: Preparing a Windows NT System for Imaging
- Example Batch File: Running the Agent Installer for Windows NT
- Example File: Configuring Machine-Specific Settings for Windows NT

Integrating with Windows NT and Symantec Ghost Process

Integrating Opsware SAS with Windows NT and Symantec Ghost follows this two-phased process:

Phase 1: Create an image

1. Manually install the Windows NT operating system on a server and customize the installation as required.

2. Run a Registry modification file from diskette that prepares the Windows NT system prior to imaging the disk. By editing the Windows NT registry, the file sets up a post-installation batch file to run when the server reboots. The batch file indirectly specifies the Opsware Agent Installer options to run and the SID and hostname changes.

   See “Example File: Preparing a Windows NT System for Imaging” on page 175 in this chapter for more information.

3. Use Symantec Ghost to take an image of the server and save the image to a network share.

Phase 2: Provision a server by using the image

1. Boot the server by using a MS-DOS boot diskette that contains Symantec Ghost (a DOS application).

When the server is running under DOS before Symantec Ghost runs, prompt the user for the Opsware Agent Installer options to run after the image is installed. Save the user input in an arguments file on the network, so that the file contains:

- Identifying information for a server
- The Opsware Agent Installer options to run on that server

See “Opsware Agent Installer Commands and Options” on page 160 in this chapter for information about a description of each option.

2. Run Symantec Ghost and install the image created in phase 1.

3. Reboot the server.

4. (AUTOMATED) The post-installation batch file runs and assimilates the server by running the Opsware Agent Installer and passing it the appropriate options.

   The post-installation batch file looks for the correct arguments file to run for that server. Each arguments file contains the MID and other identifying data of the server where it should be run. When the post-installation batch file finds the correct file, it runs the Opsware Agent Installer commands in the file.

   See “Example Batch File: Running the Agent Installer for Windows NT” on page 176 in this chapter for more information.

   The post-installation batch file can call a file that configures machine-specific settings for the NT 4 system (for example, assigns a domain-unique SID and hostname).

   See “Example File: Configuring Machine-Specific Settings for Windows NT” on page 177 in this chapter for more information.

Example File: Preparing a Windows NT System for Imaging

The following example file prepares the Windows NT system prior to imaging a disk. The file (`nt4-sys-prep.reg`) edits the Windows NT registry to call a batch file, `post-install.cmd`. The batch file is se tup to run when the server reboots after image installation.

```
nt4-sys-prep.reg
REGEDIT4
[HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
"OpswarePrep"="Z:\\tools\\post-install.cmd"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
"AutoAdminLogon"="1"
"DefaultUserName"="Administrator"
"DefaultPassword"=""
```

Example Batch File: Running the Agent Installer for Windows NT

The following example shows a post-installation batch file that runs and assimilates a server by running the Opsware Agent Installer and any other commands in the post-installation arguments file.

The example file (`post-install.cmd`) accesses a server-specific file on the network by using a server's MAC address to find the correct file.

In this example file, `%foundfile%` is the arguments file. The arguments file is copied to the file `opost.cmd` and the file is run. The arguments file contains commands such as:

```
z:\agent\agentnt.exe --template 12340002 --settime --
reconcile full
```

The short form filename, which conforms to the 8.3 DOS filename conventions, is identical to the long form filename (such as `Opsware-agent-5.1.14-win32-4.0.exe`).

```
post-install.cmd
@echo off
rem Find the appropriate post-installation arguments file
set prov_drive=z:
set params_dir=%prov_drive%\params
set tools_dir=%prov_drive%\tools

rem construct a unique temporary file name
set mac_file=%tmp%\%random%.bat
%tools_dir%\nbmac > %mac_file%
%tools_dir%\nbmac | %tools_dir%\lmod set mac_addr=[$1] > %mac_
file%
call %mac_file%
del %mac_file%
find "rem mac_addr %mac_addr%" %params_dir%\*.arg
```

```
set foundfile=
for %%i in (%params_dir%\*.arg) do call %tools_dir%\findit.cmd
%%i
if "%foundfile%"=="" goto notfound
echo Executing post-install commands from %foundfile%
copy %foundfile% %tmp%\opost.cmd
call %tmp%\opost.cmd
del %foundfile%
del %tmp%\opost.cmd
goto _end

:notfound
echo No post-install commands found for mac address %mac_addr%
goto _end

:_end
```

Example File: Configuring Machine-Specific Settings for Windows NT

The following example shows a batch file that configures machine-specific settings for an NT 4 system after the image is installed. This batch file uses third-party freeware tools to perform DOS command line parsing and reset the SID and Windows hostname.

This example batch file uses the following third-party tools:

- LMOD (available from

  home.mnet-online.de/horst.muc/)

- NEWSID (available from

  www.sysinternals.com)

```
nt4-sh.bat
@echo off
rem Find the tools
set prov_drive=z:
set tools_dir=%prov_drive%\tools
set shtmp=d:\temp

rem construct a unique hostname
echo.|time > %shtmp%\_rnd.dat
echo.|date >> %shtmp%\_rnd.dat
%tools_dir%\crc32 %shtmp%\_rnd.dat | %tools_dir%\lmod set _
hostname=OPSW-[$2] > %shtmp%\_hostname.bat
call %shtmp%\_hostname.bat
```

```
rem remove temporary files
del /f %shtmp%\_rnd.dat
del /f %shtmp%\_hostname.bat

rem change sid and hostname
%tools_dir%\newsid /a %_hostname%
```

Integration with Network Installation Management and AIX

This section provides information about how to integrate Opsware SAS with network installation management (NIM) and AIX and contains the following topics:

- Overview of Integration with NIM and AIX
- Example File: NIM Customization to Install the Opsware Agent
- Example File: NIM Customization to Increase the Partition Size

Overview of Integration with NIM and AIX

You can use AIX Network Installation Management (NIM) to manage the installation of the Base Operating System (BOS) and optional software on one or more servers running the AIX operating system.

Using NIM, you can install a group of machines with a common configuration or customize an installation for the specific needs of a given machine. The NIM environment is made up of client and server machines. A server provides resources (for example, files and programs required for installation) to another machine. A machine that is dependent on a server to provide resources is known as a client.

- For information about setting up and managing a NIM environment, *see AIX Network Installation Management Guide and Reference and NIM: From A to Z in AIX 4.3* (an IBM Corporation Redbook) documentation from IBM Corporation.
- After you integrate Opsware SAS with a NIM environment, you can use Opsware SAS to manage AIX packages and install AIX applications on servers.

See the following topics:

- See “Managing Nodes on the Software Tree” on page 255 in Chapter 10 for more information

- See “Overview of AIX Packages” on page 191 in Chapter 7 for information about how Opsware SAS manages AIX base and update filesets
- See “About AIX Patches” on page 330 in Chapter 11 for information about how Opsware SAS manages APARs

To integrate Opsware SAS with NIM and AIX, perform these tasks:

1. Copy the Opsware Agent Installer to local disk storage, for example `/var/tmp`, on the server on the which the Opsware Agent is being installed.

Copy the Opsware Agent Installer to a directory that will not be empty when the server reboots. The operating system might empty the contents of the /tmp and /var/tmp directories when the server reboots.

2. Create a NIM customization script that performs these actions:
   - Increases the partition size to accommodate the Opsware Agent
   - Invokes the Opsware Agent Installer on reboot, and then removes itself

   You can accomplish this step in any of the following ways:

   - Create a customization script to run after installation that creates a script that will run the Opsware Agent Installer after first reboot.
   - Create a customization FB script to run at first reboot that runs the Opsware Agent Installer.
   - Add the logic to run the Opsware Agent Installer and increase the partition size to an existing NIM customization script.
3. Define a NIM script resource on the NIM Master server for the customization script that you created.
4. During NIM BOS installation on a NIM client, specify the Opsware Agent customization script to run after installation.

Example File: NIM Customization to Install the Opsware Agent

The following example shows a NIM customization script that runs at the end of the NIM installation process. Running this script requires that the Opsware Agent Installer binaries are accessible in an NFS-exported directory; for example, `/export/nim/opsw_bin`.

```
#!/bin/sh
#
# Copyright (c) 2002 by Opsware, Inc
# All rights reserved.
#
# Setup Opsware Agent Installer
#

OS_VER=`uname -v`"."`uname -r`
TEMPLATE_ID="$1"

BASE=/
AGENT_SRC_DIR=/export/nim/opsw_bin
AGENT_DST_DIR=/var/lc/bootstrap
AGENT_START_SCRIPT=/etc/rc.d/rc2.d/S99zAgentInstaller
AGENT_OPTS="-os --settime --decommission --logfile
$AGENT_DST_DIR/install.log"

#
# mount the agent installer directory
#
NFS_HOST=nim.dev.opsware.com
MNT=/mnt.$$
mkdir ${MNT}
mount $NFS_HOST:$AGENT_SRC_DIR ${MNT}
AGENT_SRC_DIR=${MNT}

#
# use latest agent
#
AGENT=`ls $AGENT_SRC_DIR/opsware-agent-*-aix-$OS_VER | tail -1`
AGENT=`basename $AGENT`

if [ "$TEMPLATE_ID" ]; then
AGENT_OPTS="--template $TEMPLATE_ID --reconcile addonly $AGENT_
OPTS"
fi

echo "Agent installer version: $AGENT"
echo "Agent installer options: $AGENT_OPTS"

#
# copy over the agent installer
#
umask 022
mkdir -p $BASE/$AGENT_DST_DIR
```

```
cp $AGENT_SRC_DIR/$AGENT $BASE/$AGENT_DST_DIR/opsware-agent-
installer
chmod 555 $BASE/$AGENT_DST_DIR/opsware-agent-installer

#
# setup a start script to run the agent installer upon reboot
#
touch $BASE/$AGENT_START_SCRIPT
chmod 711 $BASE/$AGENT_START_SCRIPT
chown root:sys $BASE/$AGENT_START_SCRIPT

cat >> $BASE/$AGENT_START_SCRIPT <<EOF
#!/bin/sh

(
$AGENT_DST_DIR/opsware-agent-installer $AGENT_OPTS
rm –f $AGENT_START_SCRIPT
) 2>&1 | tee -a $AGENT_DST_DIR/`basename $AGENT_START_
SCRIPT`.log
EOF

umount ${MNT}
rmdir ${MNT}
```

Example File: NIM Customization to Increase the Partition Size

The following example shows a NIM Customization FB script that increases the partition size to accommodate the Opsware Agent on the NIM client.

```
#!/bin/sh
chfs -a size='2097152' /tmp
chfs -a size='2097152' /var
crfs -v jfs -g'rootvg' -a size='2097152' -m'/opt' -A''`locale
yesstr |
awk -F: ' {print $1}'`'' -p'rw' -t''`locale nostr | awk -F:
'{print
$1}'`'' -a frag='4096' -a nbpi='4096' -a ag='8'
mount /opt
chfs -a size='2097152' /opt
```

The part of the script that starts with `crfs` and ends with `-a ag='8'` is a single line.

Integration with Ignite-UX and HP-UX

This section provides information about how to integrate Opsware SAS with Ignite-UX and HP-UX and contains the following topics:

- Overview of Integration with Ignite-UX and HP-UX
- Example File: Ignite Configuration File
- Example File: Ignite Script to Invoke Opsware Agent Installer

Overview of Integration with Ignite-UX and HP-UX

You can use Ignite-UX to facilitate installing and recovering HP-UX on HP computer systems in your computing environment.

Ignite-UX uses configurations that control the installation of the HP-UX operating system on servers. Using Ignite-UX, you can perform the following tasks:

- Create and reuse standard system configurations.
- Archive a standard system configuration and use that archive to replicate systems.
- Create customized processes to allow interactive and unattended installs.
- Recover OS and applications after crashes and hardware failures.

After running an Ignite-UX install session, you have a working HP-UX client system.

For information about how to set up and manage Ignite-UX, see the *Ignite-UX Administration Guide* from Hewlett-Packard Company.

After you integrate Opsware SAS with an Ignite-UX system, you can use Opsware SAS to manage HP-UX packages and install HP-UX applications on servers.

See the following topics:

- See “Managing Nodes on the Software Tree” on page 255 in Chapter 10 for more information.
- See “HP-UX Packages” on page 192 in Chapter 7 for information about how Opsware SASmanages HP-UX products and filesets
- See “About HP-UX Patches” on page 331 in Chapter 11 for information about how Opsware SAS manages patch products and patch filesets

To integrate Opsware SAS with Ignite-UX and HP-UX, perform these tasks:

1. Copy the Opsware Agent Installer to local disk storage, for example `/var/tmp`, on the server on which the Opsware Agent is being installed.

Copy the Opsware Agent Installer to a directory that will not be empty when the server reboots. The operating system might empty the contents of the /tmp and /var/tmp directories when the server reboots.

2. Create a script that invokes the Opsware Agent Installer on reboot, and then removes itself.
3. Save the script on the Ignite server.
4. Create a configuration file that includes the script in a `post_config_script` clause and add the configuration file to a configuration in the Ignite configuration INDEX in the directory `/var/opt/ignite/INDEX`.

   OR

   Add a `post_config_script` clause that includes the script to an existing configuration file referenced in the Ignite INDEX.

Example File: Ignite Configuration File

The following example shows how you might create a configuration file that includes the script in a `post_config_script` clause:

```
post_config_script+=”/var/opt/ignite/scripts/add_agent_
installer”
```

Example File: Ignite Script to Invoke Opsware Agent Installer

The following example shows an Ignite script that runs at first reboot to install the Opsware Agent on a server running HP-UX.

```
#!/bin/sh
#
# Copyright (c) 2002 by Opsware, Inc
# All rights reserved.
#
# Setup Opsware Agent Installer
#
```

```
OS_VER=`uname -r | cut -c3-`
TEMPLATE_ID="$1"

BASE=/
AGENT_SRC_DIR=/var/opt/ignite/clients
AGENT_DST_DIR=/var/lc/bootstrap
AGENT_START_SCRIPT=/sbin/rc3.d/S99zAgentInstaller
AGENT_OPTS="-os --decommission --logfile $AGENT_DST_DIR/
install.log"

#
# mount the agent installer directory
#
NFS_HOST=ignite.dev.opsware.com
MNT=/mnt.$$
mkdir ${MNT}
mount -F nfs $NFS_HOST:$AGENT_SRC_DIR ${MNT}
AGENT_SRC_DIR=${MNT}

#
# use latest agent
#
AGENT=`ls $AGENT_SRC_DIR/opsware-agent-*-hpux-$OS_VER | tail -1`
AGENT=`basename $AGENT`

if [ "$TEMPLATE_ID" ]; then
AGENT_OPTS="--template $TEMPLATE_ID --reconcile addonly $AGENT_
OPTS"
fi

echo "Agent installer version: $AGENT"
echo "Agent installer options: $AGENT_OPTS"

#
# copy over the agent installer
#
umask 022
mkdir -p $BASE/$AGENT_DST_DIR
cp $AGENT_SRC_DIR/$AGENT $BASE/$AGENT_DST_DIR/opsware-agent-
installer
chmod 555 $BASE/$AGENT_DST_DIR/opsware-agent-installer

#

# setup a start script to run the agent installer upon reboot
#
touch $BASE/$AGENT_START_SCRIPT
```

```
chmod 711 $BASE/$AGENT_START_SCRIPT
chown root:sys $BASE/$AGENT_START_SCRIPT

cat >> $BASE/$AGENT_START_SCRIPT <<EOF
#!/bin/sh

case "\$1" in
start_msg)
print "Installing Opsware Agent ($AGENT):"
exit $OKAY
;;
esac
(
$AGENT_DST_DIR/opsware-agent-installer $AGENT_OPTS
rm –f $AGENT_START_SCRIPT
) 2>&1 | /usr/bin/tee -a $AGENT_DST_DIR/`basename $AGENT_START_
SCRIPT`.log
EOF

umount ${MNT}
rmdir ${MNT}
```

Chapter 7: Package Management

IN THIS CHAPTER

This chapter discusses the following topics:

Overview of Package Management

Packages are made available in Opsware SAS by uploading the packages to the Software Repository with the Opsware Command Center or by using the Opsware Command Line Interface. See “OCLI 1.0 for Package Management” on page 227 in Chapter 8 for information about for more information about Opsware Command Line Interface (OCLI).

The Opsware Command Center provides options to perform the following tasks:

- Upload packages to the Software Repository.

  The Software Repository provides a data store for all software that Opsware SAS manages. It contains packages for operating systems, applications (for example, BEA WebLogic or IBM WebSphere), databases, customer code, and software configuration information.

- Perform other package setup and management functions.

After you upload packages to the Software Repository, you install packages by adding them to nodes, assigning the nodes to servers, and reconciling the servers. Opsware SAS reconciles the differences between how a server is configured by assigned nodes and what software is actually installed. The Opsware Agent installed on each Opsware-managed server coordinates installation of software packages that are missing or need to be upgraded based on updates to nodes, and removes the packages that should no longer be installed.

See “Managing Nodes on the Software Tree” on page 255 in Chapter 10 for information about how to add software to nodes.

Opsware SAS wizards automatically assign servers to nodes and reconcile them.

Container Packages and Installable Packages

For some operating systems, the distribution or container package might contain more than one installable package. For example, Solaris packages can contain multiple installable packages, called *instances*.

When a container package is uploaded in Opsware SAS, package entries are automatically created for all the installable packages it contains.

Container packages cannot be directly attached to nodes, only installable packages. Container packages cannot be deleted directly; you can only delete the container package, and only if none of the installable packages it contains are attached to nodes.

Solaris patch clusters are an exception to this general rule. They are container packages, but can also be attached to nodes themselves.

Supported Operating Systems and Package Types

Opsware SAS will manage servers that run the following operating systems.

Each operating system that Opsware SAS supports has a list of package types that you can upload. Opsware SAS supports these package types on the supported operating systems, as the following table shows.*

Table 7-1: Supported Operating Systems and Package Types

OPERATING SYSTEM	PACKAGE TYPE	FILE FORMATS	ADDITIONAL METADATA*
AIX	LPP (contains an update fileset or base filesets)	.bff	N/A
	RPM	.rpm	N/A
HP-UX	Depot (contains products and filesets)	.tar	N/A
Linux	RPM	.rpm	N/A
Solaris	Patch	.jar, .tar, tar.gz, .tar.Z, t.gz, .zip	N/A
	Patch Cluster (contains patches)	.tar, .tar.gz, tar.Z, .t.gz, .zip	N/A
	Solaris package (contains package instances)	Datastream File	N/A
	RPM	.rpm	N/A

Table 7-1: Supported Operating Systems and Package Types

OPERATING SYSTEM	PACKAGE TYPE	FILE FORMATS	ADDITIONAL METADATA*
Windows	Hotfix	.exe	N/A
	Security Patch	.exe	N/A
	MSI	.msi	Product version and name
	OS Service Pack	.exe	Service Pack Level
	Windows Utility (Microsoft Security Baseline Analyzer and qchain)	.exe	N/A
	Microsoft Patch Database (contains a description of available patches) See “About the Microsoft Patch Database” on page 412 in Chapter 8 for more information.	.xml, .cab	N/A
	ZIP	.zip	N/A
OS Independent	Unknown	All	N/A

For certain package types, the Opsware Command Center requires that you provide additional metadata for the package.

The Build Customization Script feature is available for Linux, Solaris, and Windows.

Opsware SAS verifies that RPM files, Solaris patch clusters, AIX LPPs, Solaris packages, and HP-UX depots that are uploaded are the correct package type. You can upload packages that are designated OS Independent, but you cannot attach them to nodes.

AIX Packages

This section provides information on AIX package management within Opsware SAS and contains the following topics:

- Overview of AIX Packages
- LPP Metadata

Overview of AIX Packages

LPPs are the container packages for AIX. LPPs have the following characteristics:

- An LPP contains either one or more base filesets or an update fileset.
- When an LPP contains multiple filesets, frequently only a subset of those filesets is installed because users might want to install only certain filesets.

The basic unit of AIX packages is the fileset. Filesets have the following characteristics:

- Filesets are versioned.
- The two types of filesets are base and update.
- Users add filesets to nodes. Therefore, Opsware SAS adds filesets to and removes filesets from servers through reconcile.

Filesets are delivered as part of an LPP file, which users upload to the Software Repository. Opsware SAS automatically creates package entries for all the filesets that the LPPs contain. When viewing an LPP in the Opsware Command Center, users see which filesets it contains.

The Opsware Agent reports which filesets and Authorized Program Analysis Reports (APARs) are installed on servers because servers only report filesets and APARs (and cannot report LPPs). The Opsware Command Center shows filesets and APARs in the Installed Packages list for a server.

See “About AIX Patches” on page 330 in Chapter 11 for information about for more information about how Opsware SAS manages AIX APARs.

LPP Metadata

Opsware SAS uses the metadata contained in LPPs when creating the package entries in the list of packages. An LPP contains the following metadata:

- The name of the LPP

- The name, version, and description of each fileset in the LPP
- For an update fileset, a list of APARs addressed by the fileset
- For each APAR listed, the list of filesets that make up that APAR

Opsware SAS does not support bundles (which are abstract sets of filesets, drawn from multiple LPPs) or Program Temporary Fix (PTFs), which are similar to APARs without the metadata. However, users can still model a bundle or PTF by creating a node and attaching the filesets included in the bundle or PTF to that node.

When a user uploads an LPP, Opsware SAS performs the following actions:

- Opens the LPP and parses its metadata
- Automatically creates entries in the list of packages for the filesets in the LPP and registers them as installable
- Automatically creates entries in the list of packages for the APARs defined by the update filesets in the LPP (if any)
- Registers the LPP as a non-installable package

HP-UX Packages

This section contains the following topics:

- Overview of HP-UX Package
- Depot Metadata
- Prerequisites to HP-UX Package Management
- Example Commands: Converting a Depot
- Example File: Script to Split a Depot by Product
- Example File: Script to Split a Depot by Bundle

Overview of HP-UX Package

Depots are the container packages for HP-UX. Depots have the following characteristics:

- A depot either contains products that contain filesets, or it contains patch products that contain patch filesets.
- When a depot contains multiple products and filesets, frequently only a subset of them are installed because users might want to install only certain products or filesets.
- A depot is a special type of directory formatted for use by HP Software Distributor (SD-UX) commands. SD-UX, a software management system, is the distribution mechanism for all HP software for HP-UX.
- A depot can be a local directory, a CD-ROM, tape, or it can reside on a server on the network.
- Multiple depots can be created for different applications or purposes.
- Users upload depots to the Software Repository in TAR format.
- Users can upload depots as HP-UX 11.00 or 11.11 depots. However, HP-UX software can be compatible with both 11.00 and 11.11. When the software in a depot is compatible with both 11.00 and 11.11, upload the depot to the Software Repository for both 11.00 and 11.11.
- Depots cannot be differentiated by hardware platform, such as s700 or s800.
- HP-UX depots have two basic formats:
  - Directory – the format for depots saved on a server or CD-ROM
  - Tape – the format for standalone depot files and the format required for uploading HP-UX packages into Opsware SAS.

HP-UX depots that contain both products and patch products cannot be uploaded to a specific customer. They can only be uploaded to Customer Independent.

Products and filesets are the installable packages for HP-UX. They have the following characteristics:

- Products and filesets are versioned.
- Filesets are the smallest installable unit. A fileset can belong to only one product, but can be included in multiple subproducts or bundles.
- Subproducts are logically related filesets and are not versioned; for example, X11.Manuals.

- Products are supersets of filesets.
- Bundles are logical groups of filesets; for example, HP-UX Support Tools Bundle.

Opsware SAS supports products, filesets, and patch products as installable software.

Opsware SAS does not support bundles (which are abstract sets of filesets, drawn from depots) or subproducts by automatically creating nodes for bundles and subproducts when users upload depots. However, users can still model bundles and subproducts by creating nodes for them and attaching the filesets for the bundles and subproducts. Opsware SAS does not support using HP-UX codewords.

When a user uploads a depot, Opsware SAS performs the following actions:

- Opens the depot and parses its metadata
- Automatically creates entries in the list of packages for the products and filesets in the depot and registers them as installable
- Registers the depot as a non-installable package

If a depot contains different software for HP-UX 11.00 and 11.11, create OS-specific depots for each HP-UX version and upload the depots to the Software Repository. The Opsware Command Center does not check the OS compatibility of the products and filesets in a depot when a user uploads the depot. When attaching products or filesets to a node, the products and filesets are attachable only when the associated OS of their depot matches the OS specified for the node.

The format of HP-UX version information can be inconsistent, making it difficult to determine whether one version is older than another when installing a package that has another version already installed. Opsware SAS attempts to install it anyway. An error results if a newer version is already installed.

Opsware SAS does not provide alternate root support for HP-UX. Do not include commands that require alternate root support in the Install Flags text box of the Packages: Edit Properties page. See “Editing Package Properties” on page 217 in this chapter for more information. By default, the HP-UX `swinstall` command does *not* replace a newer version of a fileset or product with an older version. However, Opsware SAS does overwrite newer versions of filesets and products with older versions. Opsware SAS does not support relocating packages for HP-UX.

Depot Metadata

Opsware SAS uses the metadata contained in depots when creating the package entries in the list of packages. A depot contains the following metadata:

- The name, version, and description of each product in the depot
- The list of filesets in each product in the depot
- The name, version, and description of each fileset in the depot

Prerequisites to HP-UX Package Management

Before you upload a depot to the Software Repository, perform the following tasks:

1. Convert the depot on the installation media (CD-ROM) from directory format to tape format by using the `swpackage` command:

   ```
   swpackage -x media_type=tape -s <directory depot> <software
   selection> @ <file depot>
   ```

2. Split the depot into depots for each product.

You can perform this step manually by using NIM utilities or you can run a script to automate this step. See “Example File: Script to Split a Depot by Product” on page 196 in this chapter for more information. See “Example File: Script to Split a Depot by Bundle” on page 196 in this chapter for more information.

Example Commands: Converting a Depot

The following example shows the commands used to create a Quality Pack file depot from the Support Plus CD-ROM for HP-UX 11.00:

1. Mount the directory on the CD-ROM that contains the Quality Pack file depot:

```
mount -F cdfs /dev/dsk/c2t1d0 /cdrom
```

2 Convert the depot on the CD-ROM from directory format to tape format by using the swpackage command:

```
swpackage -x media_type=tape -s /cdrom/QPK1100 QPK1100 @ \
  /var/tmp/QPK1100.depot
```

Entering this command copies the QPK1100 bundle contained in the depot to a file that can be uploaded into Opsware SAS.

Example File: Script to Split a Depot by Product

```
# This is an example script that splits a depot into individual
# product depots that can then be uploaded to the Opsware
# Software Repository

for product in `swlist -l product -s <location of depot> | \
  cut -f1 | grep -v ^# | grep '[A-z]'`
do
swpackage -x media_type=tape -s <location of depot> $product \
  @ /var/tmp/$product.depot
done
```

Example File: Script to Split a Depot by Bundle

```
# This splits a depot into individual bundle depots that can
# then be uploaded to the Opsware Software Repository

for bundle in `swlist -l bundle -s <location of depot> | \
  cut -f1 | grep -v ^# | grep '[A-z]'`
do
swpackage -x media_type=tape -s <location of depot> $bundle \
  @ /var/tmp/$bundle.depot
done
```

Linux Packages

Linux packages are RPMs, which have the following characteristics:

- RPMs are both uploaded and installed as a unit so there is no distinction between container and installable packages.
- RPMs are versioned.

RPM Metadata

Opsware SAS uses the metadata contained in RPMs when creating the package entries in the list of packages. An RPM contains the following metadata - the name, version, and release of the RPM.

When a user uploads an RPM, Opsware SAS performs the following actions:

- Opens the RPM and parses its metadata
- Registers the RPM as an installable package

Solaris Packages

Solaris packages are the container packages for Solaris. Solaris packages have the following characteristics:

- A Solaris package contains one or more package instances.
- When a Solaris package contains multiple instances, frequently only a subset of those instances will be installed because users might want to install only certain instances.
- Solaris packages have two basic formats:
  - Filesystem format – the format for packages stored in a directory structure
  - Datastream format – the format for standalone package files. This format is required for uploading Solaris packages into Opsware SAS.

The basic unit of Solaris packages is the package instance. Package instances have the following characteristics:

- Package instances are versioned.
- Users add package instances to nodes. Opsware SAS adds package instances to, and removes package instances from, servers by using the reconcile function. See the *Opsware® SAS 5.2 User's Guide* for more information about Reconcile.

In the Opsware Command Center, you can upload, view, download, and delete Solaris packages, and you can view, deprecate, and attach to nodes the instances that they contain.

Opsware SAS supports Solaris packages in the following ways:

- Users upload Solaris packages in the uncompressed datastream file format.

- Opsware SAS can install interactive and non-interactive Solaris package instances. Interactive Solaris package instances require response files.
- Opsware SAS displays the name and version number for Solaris packages in the following way:

  ```
  SUNW125f-1.0,REV=2001.03.21.17.00
  SUNW1394h-11.9.0,REV=2002.04.06.15.27
  ```
- The Solaris utilities (such as `pkgadd`) use an admin file. The admin file stores settings regarding how the utilities should work. Each Opsware Agent on managed servers includes its own admin file that it uses when installing Solaris package instances. The admin file that the Opsware Agent uses is *only* used by Opsware SAS and does *not* set defaults for other applications using `pkgadd`.
- In some instances, a Solaris package might only get partially installed. A partial installation generally occurs when a package contains an installation script (other than the checkinstall script - for example, a preinstall or postinstall script) and that script exits non-zero during package installation. A partially installed Solaris package can be removed as if it were installed as a full package by removing it, or by overwriting it with a new package.
- For more information on `pkginfo, pkgadd, and pkgrm,` see the man pages.

Response files are text files. The entries in a response file occur as name = value pairs; for example, `BASEDIR="/opt/SUNWexplorer"` is a valid entry.

Opsware SAS supports response files in the following ways:

- Users create response files outside of Opsware SAS by using the `pkgask` Solaris utility.
- By using the Package Properties page in the Opsware Command Center, users upload, overwrite, view, and delete response files that are associated with Solaris package instances.
- Each response file is accessible *only* in the context of the Solaris package instance to which it belongs.
- Each Solaris package instance can have zero or one response file. Response files are not shared by different Solaris package instances.
- Attaching an interactive package to a node includes the response file because Opsware SAS stores the response file with the package. You do not need to attach the response file to the node.

- After a Solaris package instance has a response file, Opsware SAS uses that response file whenever the Solaris package instance is installed.
- If a Solaris package instance requires a response file and that file is missing in the Opsware Command Center, Opsware SAS might report an error when any server is reconciled with that Solaris package instance.

When a user uploads a Solaris package, Opsware SAS performs the following actions:

- Opens the package and parses its metadata
- Automatically creates entries in the list of packages for the package instances in the package and registers them as installable
- Registers the Solaris package as uninstallable

Solaris Package Metadata

Opsware SAS uses the metadata contained in Solaris packages when creating the package entries in the list of packages. A Solaris package contains the following metadata - the name, version, and description of each package instance in the package.

Prerequisites to Solaris Package Management

The Solaris package must be in datastream format before you can upload it to the Opsware Software Repository. If it is in file system format, you can convert it by using the `pkgtrans` command:

```
pkgtrans -s <location of package> <new package> all
```

Windows Packages

Opsware SAS supports the following Windows packages:

- Microsoft Installer Packages
- Microsoft Hotfixes, Security Patches, and Service Packs

Microsoft Installer Packages

Microsoft Installer packages (MSI) have the following characteristics:

- Contain all the information that the Microsoft Installer requires to install an application or product
- Contain information that the installer requires to run the setup user interface

MSI packages contain:

- An installation database
- A summary information stream
- Data streams for various parts of the installation

Opsware SAS supports .msi files as installable software.

MSI Package Metadata

Opsware SAS catalogs each MSI package by its ProductName and ProductVersion. These properties are defined in the Properties table of the MSI installation database. When you upload an MSI package to Opsware SAS, you are required to provide ProductName and ProductVersion exactly as they appear in the Properties table.

To discover the ProductName and ProductVersion, use the Orca tool that Microsoft provides as part of its MSI SDK, available for download from

www.microsoft.com

Perform the following steps to discover the ProductName and ProductVersion of an MSI package:

1. Launch the Orca application.
2. Select File ➤ Open to open the target MSI package file.
3. In the Tables Column, select Property.
4. Note the exact value for the ProductName and ProductVersion properties.

Prerequisites to MSI Package Management

Opsware SAS supports the Microsoft Windows Installer versions 1.1 and 2.0. Version 1.1 is included with Windows 2000, and version 2.0 is included with Windows 2003.

Windows NT does not include a version of the Windows Installer, but the Microsoft Windows redistributable can be obtained for download at http://www.microsoft.com or by including the `--withmsi` option on the Opsware Agent Installer command line.

See the *Opsware® SAS 5.2 User's Guide* for more information about the steps to install an Opsware Agent on a server.

Microsoft Hotfixes, Security Patches, and Service Packs

These packages include:

- Hotfixes
- Service Packs
- Security Patches

Hotfixes are issue specific and should only be applied if you experience the exact issue addressed by the hotfix, and only if you are using the current operating system version that has had the latest service pack applied.

Service packs are groups of hotfixes. They are more thoroughly tested than individually-released hotfixes, and are available to all customers, not just those with the specific problem.

Security patches are similar to hotfixes, but are mandatory if you are experiencing the specific problem they are created to address, and they need to be deployed as soon as they are made available.

Microsoft Patch Metadata

When you upload a Service Pack, Opsware requires the user to provide the version of the service pack. When you upload Hotfixes and Security Patches, Opsware requires the user to provide the operating system version and the patch type.

ZIP Packages

This section provides information on ZIP package management within Opsware SAS and contains the following topics:

- ZIP Package Support
- ZIP Packaging
- Creating ZIP Packages
- Uploading ZIP Packages
- Defining Package Installation and Remove Scripts
- Editing Properties for ZIP Packages
- Info-Zip Compatible ZIP Packages
- Windows Performance for Uploading Packages

ZIP Package Support

The Opsware Command Center adds support for ZIP packages on the following operating systems:

- Windows NT4
- Windows 2000

ZIP Packaging

Use ZIP packages primarily to deliver code that can be run on a server. You can also use them to deliver application files for installing applications.

When a user installs a ZIP package on a server, the files are automatically extracted and saved to a directory that the user selects; otherwise, a default directory is used. Opsware SAS keeps track of all ZIP packages that it has installed, which prevents you from installing a ZIP package with the same name twice.

A ZIP package has no limits or restrictions on the size, format, or number of files that it contains.

Opsware SAS supports ZIP encapsulation for application package files that were built using other standalone installation programs, for example, InstallShield.

Opsware SAS requires silent install operation for programs designed for interactive installation. When you package these program files to upload to Opsware SAS, use the silent install options to play back automatic responses to provide unattended installation.

For information on how to construct ZIP files that use silent install features for unattended installation operations, refer to the documentation provided with the archive program that you are using.

Creating ZIP Packages

Opsware SAS supports the ZIP file format for application package files that are built using non-MSI standalone installation programs, for example, InstallShield. Programs such as InstallShield were originally designed to provide for interactive installation. However, using the silent install feature, InstallShield users can play back a recording of a previous application installation that creates an unattended installation file with a suffix ISS.

The interactive installation recording is saved in the form of a setup.iss file that contains the responses to the interactive dialog boxes and popup menus that typically display during an interactive installation. After the response file is recorded, you can pass the setup.iss file as an argument to setup.exe executed from the command line to perform an unattended installation.

Similarly (using InstallShield), uninstalling an application can be set up to run unattended using the UnInst.exe command invoked with the -a and -y options to instruct the installer to run uninstall in silent mode.

See the documentation provided with your specific installer software for more information on silent install features and options.

Uploading ZIP Packages

You can upload, re-upload, download, delete, deprecate, and attach ZIP packages to nodes with the Opsware Command Center. You can also use the Opsware Command Line Interface (OCLI) to upload and download ZIP packages.

Enter Windows ZIP file as the value for the `--pkgtype` argument to upload a ZIP package by using the OCLI.

See “OCLI 1.0 for Package Management” on page 227 in Chapter 8 for more information.

Defining Package Installation and Remove Scripts

Because you can invoke silent installation and uninstallation from the command line, you can create scripts that perform silent installation and uninstallation. You can then include the scripts as part of the package file properties that you specify when you upload a ZIP file to the Software Repository.

Editing Properties for ZIP Packages

After you upload a ZIP package to the Software Repository, the Opsware Command Center displays a page in which you can enter additional package properties. On the Edit Properties page, you can define scripts to run when you install or uninstall ZIP packages.

Perform the following steps to edit the properties for a ZIP package as defined in Opsware SAS:

1 Click the ZIP package link for the package that you want to edit. The Manage Packages: Edit Properties page appears.

The Manage Packages: Edit Properties page for ZIP packages does not include the Install and Remove Flags text boxes.

2 Enter an installation directory in the Installation Directory text box. The default installation directory, if nothing is entered, is `%SystemDrive%\Program Files\[basename of ZIP file]`.

When you specify the installation directory, post-installation, and pre-uninstallation script names for a ZIP package, do not use quotation marks to enclose the entire directory path and the script names.

When you uninstall a ZIP package, the extracted ZIP files that were installed on the server are not removed from the server. To uninstall those files, you must run an uninstallation script by specifying that script in the Pre-Uninstall Script Filename text box.

3 Configure the location of the post-installation or pre-uninstallation scripts and enter the script names in the Post-Install Script Filename or Pre-Uninstall Script Filename text boxes. The installation and uninstallation scripts must be included in the ZIP archive.

4 Click the **If non-zero return status, halt operation** check box for either the installation or uninstallation so that the script stops when it fails.

Extracting a ZIP package fails if the top-level directory in the file's pathname does not exist.

Info-Zip Compatible ZIP Packages

Opsware SAS offers package management support for Info-Zip compatible.zip packages. The files that are archived within Info-Zip are installable files on Opsware SAS. You can download the.zip package creation tool from

www.info-zip.org

Info-Zip Compatible Package Metadata

Opsware SAS uses the ZIP package filename to uniquely identify a ZIP package.

Prerequisites of Info-Zip Compatible Package Management

Full support for managing ZIP packages on a server is included with the Windows Opsware Agent.

Windows Performance for Uploading Packages

When you upload packages from a Windows computer, users can improve the performance of the computer used to upload by changing TCP stack registry settings that affect upload speeds. The recommended change to the Windows registry file increases the default tcp-send buffer size from 8 KB to 16 KB.

Consult your system administrator before you make this change.

Perform the following steps to change the tcp-send buffer setting:

1. Using regedit, navigate to the following registry key:

```
HKEY_LOCAL_MACHINE
  SYSTEM
    CurrentControlSet
      Services
        Afd
          Parameters (Create this key if it does not already
exist)
```

2. Set the following value for the key:

```
Name: DefaultSendWindow
Value Type: REG_DWORD
Value: 16384 (decimal)
```

After you set the value, reboot the machine for the changes to take effect.

Overview of Package Management Tasks

The Package Management feature of Opsware SAS provides tools for defining package types and uploading packages into Opsware SAS. The tasks that you can perform when you use this feature include:

- Displaying Packages
- Searching for Packages

- Viewing Packages Assigned to Nodes
- Uploading a Package
- Overwriting a Package
- Editing Package Properties
- Deleting a Package
- Deprecating a Package
- Downloading a Package

Displaying Packages

By default, the Opsware Command Center displays results (up to 10 package listings per page) in alphabetical order by name. Links to consecutive pages (if there are more than 10 packages to display) are provided at the bottom of the page. In addition, you can click the Show All link to display up to 500 packages at a time in a scrollable list.

You can also sort the results of the packages display by clicking any column heading, for example, Name, Description, or OS Version, to sort the list by that column and toggle the display of packages between ascending and descending order.

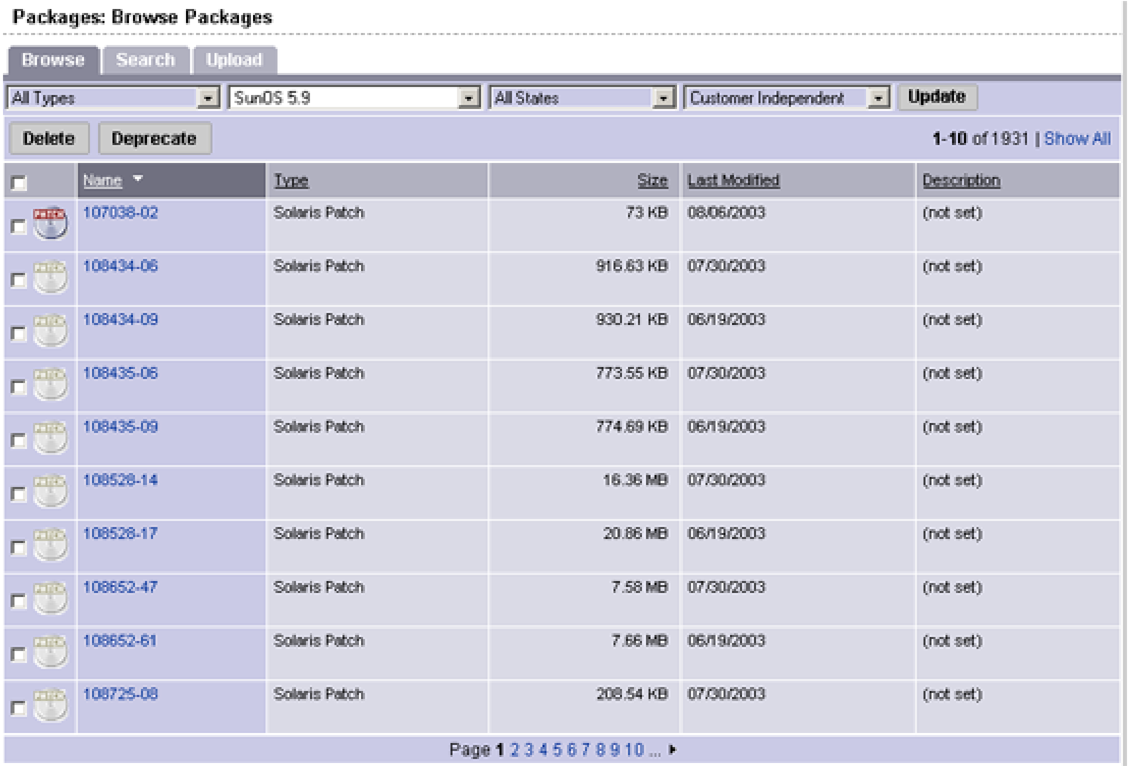
Perform the following steps to display results:

1 From the navigation panel, click Software ➤ Packages.

You can also use the Search option in the navigation panel to search for specific package names or locate packages for specific customers.

The Packages: Browse Packages page appears that lists packages available in the Software Repository. By default, the Packages page displays only the packages that the user has permission to view, as Figure 7-1 shows. Packages are associated with customers and users are given permission to manage resources for specific customers in Opsware SAS.

Figure 7-1: Packages: Browse Packages Page



Packages: Browse Packages

All Types | SunOS 5.9 | All States | Customer Independent

1-10 of 1931 | Show All

□	Name	Type	Size	Last Modified	Description
□	107038-02	Solaris Patch	73 KB	08/06/2003	(not set)
□	108434-06	Solaris Patch	916.63 KB	07/30/2003	(not set)
□	108434-09	Solaris Patch	930.21 KB	06/19/2003	(not set)
□	108435-06	Solaris Patch	773.55 KB	07/30/2003	(not set)
□	108435-09	Solaris Patch	774.69 KB	06/19/2003	(not set)
□	108528-14	Solaris Patch	16.36 MB	07/30/2003	(not set)
□	108528-17	Solaris Patch	20.86 MB	06/19/2003	(not set)
□	108652-47	Solaris Patch	7.58 MB	07/30/2003	(not set)
□	108652-61	Solaris Patch	7.66 MB	06/19/2003	(not set)
□	108725-08	Solaris Patch	208.54 KB	07/30/2003	(not set)

Page **1** 2 3 4 5 6 7 8 9 10 ... ▸

For each package available for a selected customer, operating system, type, and state, the Opsware Command Center displays the package's name, size, last modified date, and description, in addition to the selected operating system and customer.

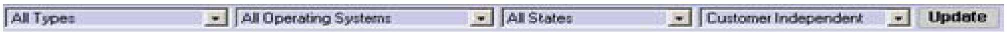
2 To display the properties of the package, click the package name.

See "Editing Package Properties" on page 217 in this chapter for more information.

Details: Filtering the Packages to Display

The top panel of the page displays four filters that you can specify to qualify the packages that the Opsware Command Center displays, as Figure 7-2 shows.

Figure 7-2: Filters for Selecting Packages to Display



- Package Type – specifies the package type for the operating system that you select.
- Operating System – specifies the operating system for which packages are available. You can select All Operating Systems or choose specific operating systems.
- Package State – specifies whether the display lists all packages or only those that are available or deprecated. By default, the Opsware Command Center shows all packages. Selecting *Deprecated* from the list displays only those packages that are deprecated in the Software Repository. Selecting *Available* displays only those packages that are not deprecated.
- Customer – specifies the customer for which packages are available. Options for customer selections are those that your Opsware administrator defines by using the Opsware Administration feature from the navigation panel.

Searching for Packages

Knowing how package names are defined helps you perform more precise searches. For example, the package name:

```
iPlanet_Web_Server-4.1sp9-LC~0.sparc64.rpm
```

specifies a package that contains iPlanet Web Server software, version 4.1sp9, running on the Sun Solaris operating system.

Perform the following steps to search for packages:

1 From the navigation panel, click Software ➤ Packages.

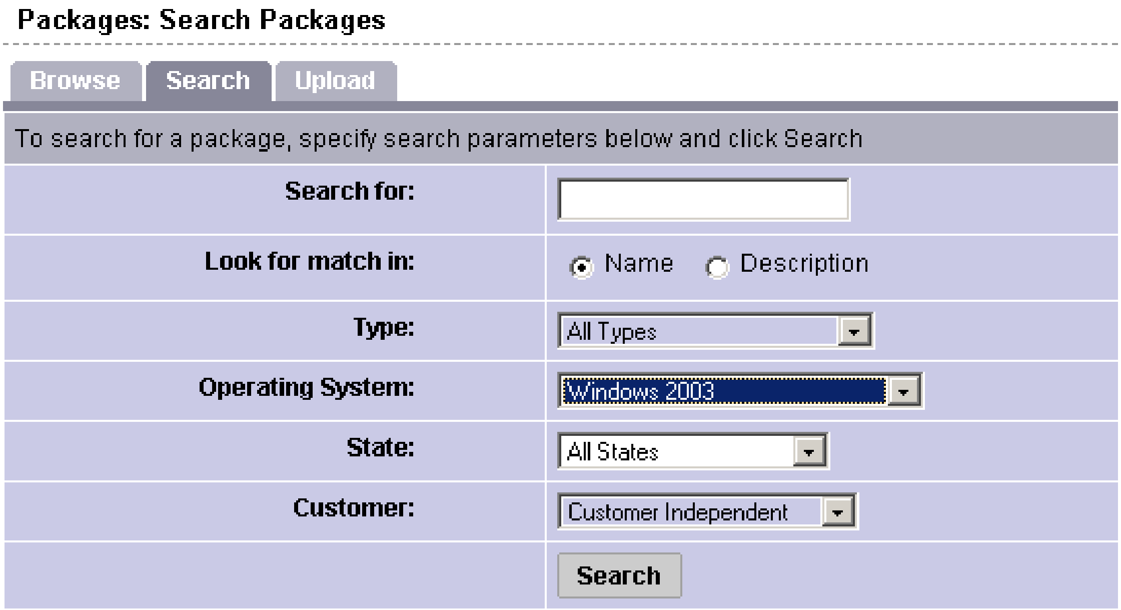
You can also use the Search options in the navigation panel to search for specific package names or locate packages for specific customers.

The Packages: Browse Packages page appears that lists the packages in the Software Repository that match the criteria set by the filters at the top of the page.

By default, the packages display for the customer with whom the user is associated.

2 Click the Search tab. A search form appears in which you can enter more specific criteria to locate packages, as Figure 7-3 shows.

Figure 7-3: Searching for Packages



Packages: Search Packages

To search for a package, specify search parameters below and click Search

Search for:	
Look for match in:	● Name ○ Description
Type:	All Types
Operating System:	Windows 2003
State:	All States
Customer:	Customer Independent

3 Enter your search criteria:

- In the Search for field, enter a simple text string to match the name or description of specific packages. You can also specify wildcard characters to match multiple characters as part of the search string. (The Opsware Command Center automatically adds a "*" wildcard character after any text string you specify, if you do not specify any wildcards in your search string.)
- Select a Look for match in option button to specify whether to match a text search string in a package's name or description (that was entered in the Package Properties page).
- Restrict your search by package type, operating system, file state, and customer:
    - Type – specifies the package type for the operating system selected. By default, all package types display.
    - Operating System – specifies the operating system for which packages are available. You can select All Operating Systems or choose specific operating system.

- State – specifies whether the display lists all packages or only those that are available or deprecated. By default, the Opsware Command Center shows all packages. Selecting Deprecated from the list displays only those packages that are deprecated in the Software Repository. Selecting Available displays only those packages that are not deprecated.
- Customer – specifies the customer for which packages are available. Options for customer selections are those that your Opsware administrator defines by using the Opsware Administration channel.

4 Click the Search button. The Opsware Command Center returns a list of packages that match the search criteria that you specified.

5 Click a package name to view the package properties.

OR

Click the Return to Search Packages hyperlink.

Viewing Packages Assigned to Nodes

Perform the following steps to view packages that are assigned to nodes:

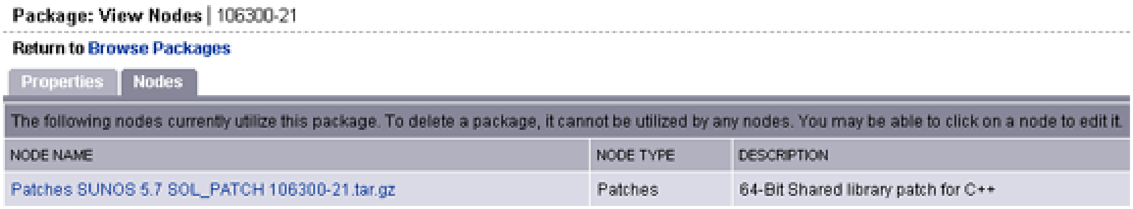
1 Locate the package whose attachment to nodes you want to view. Locate the package either by browsing (See “Displaying Packages” on page 206 in this chapter for more information) or by searching (See “Searching for Packages” on page 208 in this chapter for more information).

2 Click the package name link for the package whose attachment to nodes you want to view. The Packages: Edit Properties page appears.

3 Click the Nodes tab. The Package: View Nodes page appears. The page displays the nodes to which the package is already attached, as Figure 7-4 shows.

If you are viewing the properties for an AIX LPP, Solaris package, Unknown package, Windows utility, Microsoft Patch Database, Build Customization Script, or HP-UX depot, the Nodes tab does not appear because these packages cannot be attached to nodes.

Figure 7-4: Viewing Packages Attached to Nodes Page



Package: View Nodes | 106300-21

Return to Browse Packages

The following nodes currently utilize this package. To delete a package, it cannot be utilized by any nodes. You may be able to click on a node to edit it.

NODE NAME	NODE TYPE	DESCRIPTION
Patches SUNOS 5.7 SOL_PATCH 106300-21.tar.gz	Patches	64-Bit Shared library patch for C++

4. (Optional) Click the node name to edit the node. For example, you can edit the node to remove the package.

You cannot add deprecated packages to nodes.

Uploading a Package

Each operating system supported by Opsware SAS supports certain package types. See "Overview of Package Management" on page 187 in this chapter for more information.

If a package that is being uploaded already exists in the Software Repository, Opsware SAS overwrites the package. See "Overwriting a Package" on page 216 in this chapter for more information.

If you upload Solaris patch clusters that contain patches that already exist in the Software Repository, the patches are overwritten. However, Opsware SAS preserves any reboot options or flags set for the patches in the Opsware Command Center.

If an update fileset is part of many different APARs, Opsware SAS can take a long time to upload the LPP that contains it, because it must create a large number of APARs in the list of packages. The package upload can appear to time-out in the Opsware Command Center. However, Opsware SAS continues to upload the package.

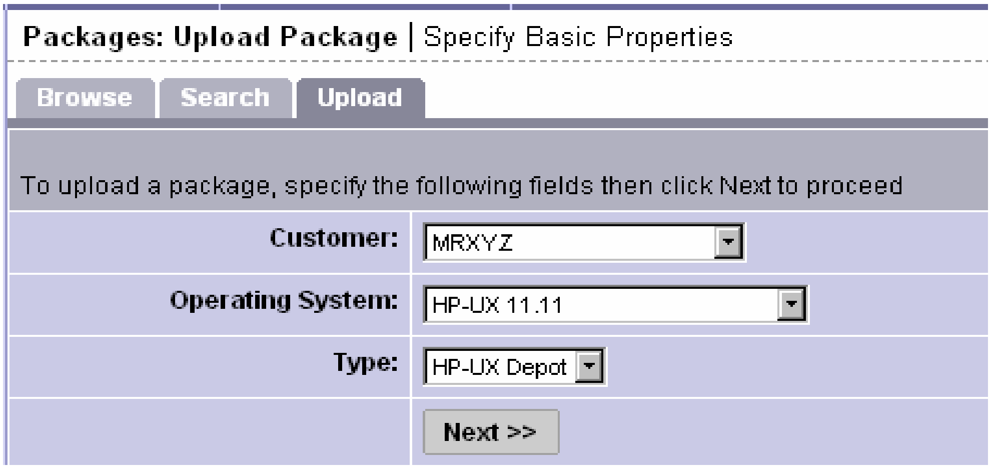
When you upload a Windows MSI package, the information that you enter about the package must match the internal data (ProductName and ProductVersion) stored in the file or Opsware SAS reports errors when the package is installed on servers.

To obtain the ProductName and ProductVersion from an MSI package, use the Orca tool from Microsoft Corporation. You can download this tool as part of the MSI software developers' kit (SDK) v1.2. See "MSI Package Metadata" on page 200 in this chapter for information about how to obtain and use Orca.

Perform the following steps to upload a package:

1. From the navigation panel, click Software ➤ Packages. The Packages: Browse Packages page appears.
2. Click the Upload tab. The Packages: Upload Package page appears, as Figure 7-5 shows.

Figure 7-5: Packages: Upload Package, Specify Basic Properties Page



Packages: Upload Package | Specify Basic Properties

To upload a package, specify the following fields then click Next to proceed

Customer: MRXYZ

Operating System: HP-UX 11.11

Type: HP-UX Depot

3. Specify the operating system and customer for which the package is to be used:

   Customer - specifies the customer for which packages will be used. Options for customer selections are those that your Opsware administrator defines by using the Opsware Administration feature from the navigation panel.

   When you upload any patch, Windows utility, or Microsoft Patch database, the file is automatically associated with Customer Independent regardless of the customer that you select from the drop-down list. HP-UX depots that contain both products and patch products cannot be uploaded to a specific customer. They can only be uploaded to Customer Independent.

Operating System - specifies the operating system for which the package is to be used. You can select from specific operating systems.

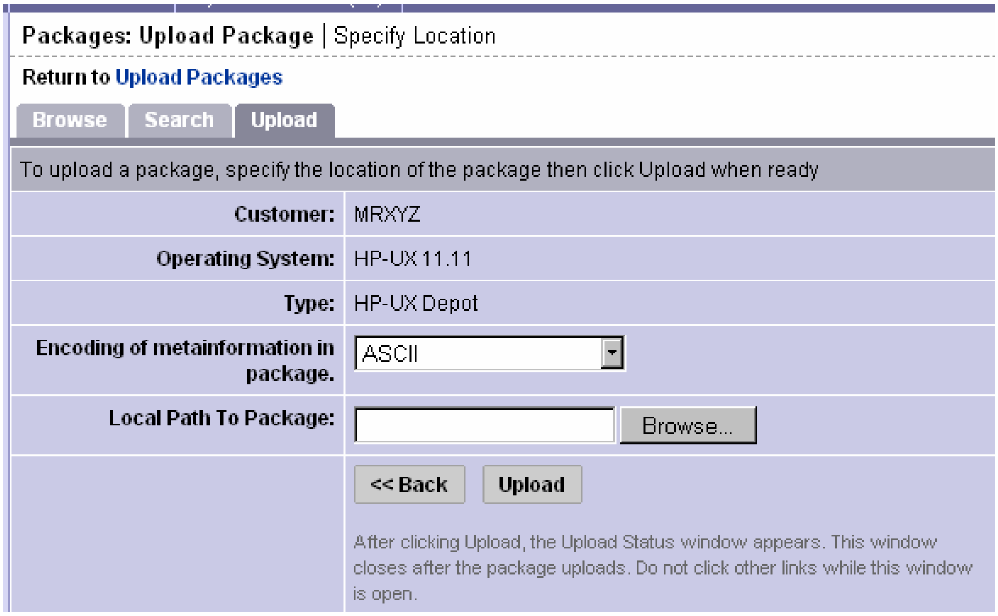
When you select a Windows utility or Microsoft database, the operating system is automatically set to Windows 2000.

Type - specifies the package type for the operating system selected. Certain package types, for example, patches or Windows utilities, force the customer to be Customer Independent.

Opsware SAS verifies that RPMs, Solaris patch clusters, AIX LPPs, Solaris packages, and HP-UX depots uploaded are the correct package type.

4 Click the Next button. If you select Windows MSI or OS Service Pack as the package type, a second form appears that prompts you to enter additional metadata for the package, as Figure 7-6 shows.

Figure 7-6: Packages: Upload Package Specify Location Page



Packages: Upload Package | Specify Location

Return to Upload Packages

To upload a package, specify the location of the package then click Upload when ready

Customer:	MRXYZ
Operating System:	HP-UX 11.11
Type:	HP-UX Depot
Encoding of metainformation in package.	ASCII
Local Path To Package:	

After clicking Upload, the Upload Status window appears. This window closes after the package uploads. Do not click other links while this window is open.

5 If necessary, enter additional required information for the package and click the Next button. A page appears that prompts you to specify the location of the package file.

- In the **Local Path to Package** field, enter the name and directory location of the package that you want to upload or click the Browse button to locate and select the package to upload.
- In the **Encoding of metainformation in package** field, select the encoding scheme to be used by the package.

You need to specify an encoding scheme so that Opsware SAS can extract the metadata contained in the package and correctly display the information in non-ASCII characters in the Opsware Command Center (for example, in the Package Properties pages).

6 Click the Upload button.

If a package (excluding AIX LPPs, HP-UX depots, and Solaris packages) with the same name already exists in the Software Repository for the same customer and operating system, the Opsware Command Center overwrites the existing file after it prompts you to confirm your choice. See “Overwriting a Package” on page 216 in this chapter for more information.

After you upload the package, the Opsware Command Center displays a page where you can enter additional package file property information.

If you are uploading a Solaris package, you can upload a response file for each of its instances by editing the response file's package properties for those instances.

See “Editing Package Properties” on page 217 in this chapter for information about additional properties that you can specify and the steps to upload a response file for a Solaris package instance.

Encoding Schemes for Package Metadata and Scripts

In Opsware SAS, you can specify encoding schemes for package metadata and scripts in the following ways:

- Specify the encoding scheme for package metadata when uploading packages in the Opsware Command Center (in the Packages feature in the navigation panel and Software Install Wizard) or by using the Opsware Command Line Interface (OCLI).

When specified, the Opsware Command Center correctly displays in non-ASCII any package metadata, description fields, and error and status message returned by the operating system of the managed servers.

- Specify the encoding scheme for scripts when uploading them in the Opsware Command Center (in the Run Distributed Script Wizard and Scripts channel).

  A user must specify an encoding scheme for an uploaded script so that Opsware SAS can convert the bytes inside the script into UTF-8 format by using the encoding scheme with which the script was created.

  After scripts run, users can download a ZIP file that contains the results encoded in UTF-8 format.

  For example, on Unix operating systems, you can use iconv (the code set conversion function) to interpret the downloaded results of the script execution.

The Opsware Command Center includes the following selections for encoding schemes:

- ASCII
- BIG5
- BIG5-HKSCS
- CP850, CP862, CP866, CP874, CP932, CP949, CP950, CP1133, CP1250, CP1251, CP1252, CP1253, CP1254, CP1255, CP1257, CP1258, CP1266
- EUC-CN, EUC-JP, EUC-KR, EUC-TW
- GB18030, GBK
- GEORGIAN-ACADEMY
- GEORGIA
- N-PS
- HZ
- ISO-2020-CN, ISO-2020-CN-EXT, ISO-20202-KR, ISO-2022-JP, ISO-8859-1, ISO-8859-2, ISO-8859-3, ISO-8859-4, ISO-8859-5, ISO-8859-6, ISO-8859-7, ISO-8859-8, ISO-8859-9, ISO-8859-10, ISO-8859-13, ISO-8859-14, ISO-8859-15, ISO-8859-16
- JOHAB
- KOI8-R, KOI8-RU, KOI8-T, KOI8-U
- MULELAO-1

- SHIFT_JIS
- TCVN
- TIS-620
- UCS-2, UCS-4
- UTF-8
- VISCII

Overwriting a Package

You can overwrite an uploaded package with a new package that has the same name (the contents of the package might be different.) The new package keeps the same property information as the current uploaded package and the same nodes to which the current package is already assigned or attached.

You *cannot* overwrite container packages (LPPs, HP-UX depots, or Solaris packages). To update a container package in the Opsware Command Center, delete the existing package and upload the file again. You can only delete the container package if none of its installable packages are attached to nodes.

When you overwrite a package, Opsware SAS deletes the existing package and uploads the new package. If you have manually changed any configuration in the package on a server, those changes are removed when you reconcile the server. Opsware SAS removes manual changes because the package was upgraded with a new version.

If you upload a Solaris patch cluster that contains patches that already exist in the Software Repository, the patches are overwritten. However, any reboot options or flags set for the patches in the Opsware Command Center are not affected.

See “Editing Package Properties” on page 217 in this chapter for more information.

Perform the following steps to overwrite a package:

1. Locate the package that you want to replace with a newer version. Locate the package by browsing (See “Displaying Packages” on page 206 in this chapter for more information) or by searching (See “Searching for Packages” on page 208 in this chapter for more information).

2 Click the package name link for the package that you want to overwrite. The Packages: Edit Properties page appears.

3 Click the Replace button at the bottom of the page. The Packages: Upload Package page appears.

4 In the Local Path to Package field, enter the name and directory location of the newer package you want to upload.

OR

Click the Browse button to locate and select the package to upload.

5 Click the Upload button.

Editing Package Properties

After you upload a new file or select an existing package in the Software Repository, the Opsware Command Center displays a page that you can use to add or update additional package properties.

You *cannot* change the operating system or customer association of a package by editing the package properties.

Perform the following steps to edit package properties:

1 Locate the package whose properties you want to edit. Locate the package by browsing (See "Displaying Packages" on page 206 in this chapter for more information) or by searching (See "Searching for Packages" on page 208 in this chapter for more information).

2 Click the package name link for the package that you want to edit. The Packages: Edit Properties page appears.

Some of the properties fields discussed in Step 3 might not appear on the page because the fields and information that appear are based on package type.

3 Edit the following properties for the package:

- Description – specifies a short description that is used to indicate the package's contents.

- Upgradable – allow the RPM to be installed with the -U option, which removes the old version of the RPM and installs the new version in a single step. By default, the Upgradable checkbox is selected. The -U option is used in the following two cases. First, the RPM is upgradable, a version of the RPM has already been installed, but not with Opsware SAS, and the installed version has not been adopted by Opsware SAS. Second, the RPM is upgradable, one or more versions of the RPM have already been installed with Opsware SAS, these versions are upgradable, and these versions are slated to be removed during this reconcile operation. In other cases, even if the Upgradable checkbox is selected, the RPM is installed with the -i option.
- Install Flags – optional arguments that you can specify to run when this package is installed on servers (a node that includes this package is assigned to a server and the server is reconciled).
- Pre-Install Script – enter the script required to run before you install the package.
- End this and subsequent installs if this script fails – select this option if you want this and all other installations to stop if this script fails.
- Post-Install Script – enter the script required to run after you install the package.
- End subsequent installs if this script fails – select this option if you want to end all installations if this script fails.
- Reboot on Successful Install – click this option if you want the system to reboot when the package is successfully installed.
- Uninstall Flags – optional arguments that you can specify to run when this package is uninstalled (a node including this package is removed from a server and the server is reconciled).
- Pre-Uninstall Script – enter the script required to run before the package is uninstalled.
- Post-Uninstall Script – enter the script required to run after the package is uninstalled.
- Reboot on Successful Uninstall – click this option if you want the system to reboot when the package is successfully uninstalled.

You must specify valid command line options in the Install and Uninstall Flags text boxes. Specifying invalid command line options in these text boxes can cause package installations and uninstallations to fail when Opsware users reconcile servers. Scripts must likewise be entered with care for the same reason.

Do not use quotation marks to enclose directory paths or script names or the installation will fail.

- Deprecated – optional selection that you can use to deprecate a package uploaded in the Software Repository. After you deprecate a package, it is no longer available to be added to new nodes.
- Notes - Enter any notes about the installation or uninstallation.

For Windows ZIP Files:

Unlike the previous fields, the name of the script file is entered here, not the script itself. Also, the Install Flags and Uninstall Flags fields do not appear for this type of file.

- Installation Directory — enter the path where you will install the ZIP file. If you do not enter a path, the default directory is `%SystemDrive%\Program Files\[`*`basename of zip file`*`]`.
- Post-Install Script Filename — enter the name of the post-installation script included in the archive being installed.
- Pre-Uninstall Script Filename - enter the name of the pre-uninstallation script included in the archive being uninstalled.

Through the Edit Properties page, you can upload, delete, and overwrite response files for Solaris package instances. The buttons to manage response files only appear when you are viewing the properties for a Solaris package instance.

4 To upload a response file for a Solaris package instance, follow these steps:

1. Click the Upload button in the Response File field. This button and field only appear for Solaris package instances. A popup window appears that prompts you to specify the path for the response file.
2. Specify the file path by entering it in the text box or browsing.

3. Click the Upload button. The popup window closes and the response filename appears in the page.

See "Solaris Packages" on page 197 in this chapter for information about how to use response files with Solaris package instances.

5 To delete a response file for a Solaris package instance, click the Delete button in the Response File field. This button and field only appear for Solaris package instances.

6 To overwrite a response file for a Solaris package instance, click the Replace button and specify the path to the new file. The file can have the same name or a different filename as the existing file. Opsware SAS replaces the response file with the new file.

7 Click the Save button.

You can also replace (overwrite), delete, or download a package directly from the Edit Properties page.

Deleting a Package

You can delete packages so that they are no longer available to add to nodes. The ability to delete a package depends on the package type that you select.

Deleting a Solaris patch cluster does *not* delete the patches contained in the cluster from the Software Repository.

When you delete a Solaris package instance, any response file associated with the package is also deleted.

Restrictions on Deleting Packages

You cannot delete packages if the following conditions are true:

- The package is attached to a node.
- The package is attached to a patch node that has a server also attached.
- The package is attached to a patch node that is in a template.
- Any of the items contained in a package are attached to a node.
- The user does not have permission to access the resources for that customer.
- The package type is not a physical package type.

- The package type is not deletable because the system needs it.
- The package contains a package that is attached to a patch node that has a server also attached.
- The package contains a package that is attached to a patch node that is in a template.

Do *not* delete a Solaris patch when the patch is contained in a Solaris patch cluster. Deleting a Solaris patch contained in a Solaris patch cluster can cause problems when you install the patch cluster on a server.

Opsware, Inc. recommends that you do not delete packages that have been installed on the servers by Opsware SAS. Deleting such a package that is in use can cause problems in Opsware SAS.

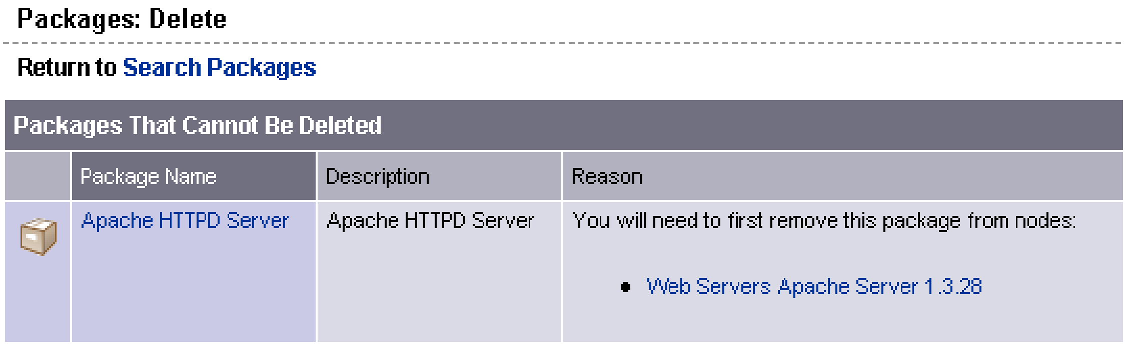
Perform the following steps to delete a package:

1. From the navigation panel, click Software ➤ Packages. The Packages: Browse Packages page appears.
2. Select the check boxes next to the packages that you want to delete.

   You can also click the check box at the beginning of the list to select or clear package selections.
3. Click the Delete button. A confirmation page appears that prompts you to confirm the deletion.

The Opsware Command Center also indicates whether packages selected for deletion are still assigned to nodes. To delete packages, you must remove the packages from assigned nodes before you delete them, as Figure 7-7 shows.

Figure 7-7: Attempting to Delete a Package Attached to a Node



Packages: Delete

Return to Search Packages

Packages That Cannot Be Deleted

	Package Name	Description	Reason
	Apache HTTPD Server	Apache HTTPD Server	You will need to first remove this package from nodes: • Web Servers Apache Server 1.3.28

4 Click the Delete button to remove the packages from the Software Repository.

Deprecating a Package

You can deprecate packages so that they are no longer available to add to nodes. The ability to deprecate a package depends on the package type that you select.

Deprecating an APAR does not deprecate the update filesets within it. Conversely, deprecating an update fileset does not deprecate the APARs of which the update fileset is a part. If a user reconciles a node for an APAR that contains a deprecated update fileset, Opsware SAS installs the deprecated fileset. Additionally, users can install available update filesets for deprecated APARs. See “AIX Packages” on page 191 in this chapter for more information. See “About AIX Patches” on page 330 in Chapter 11 for information about how Opsware SAS manages APARs.

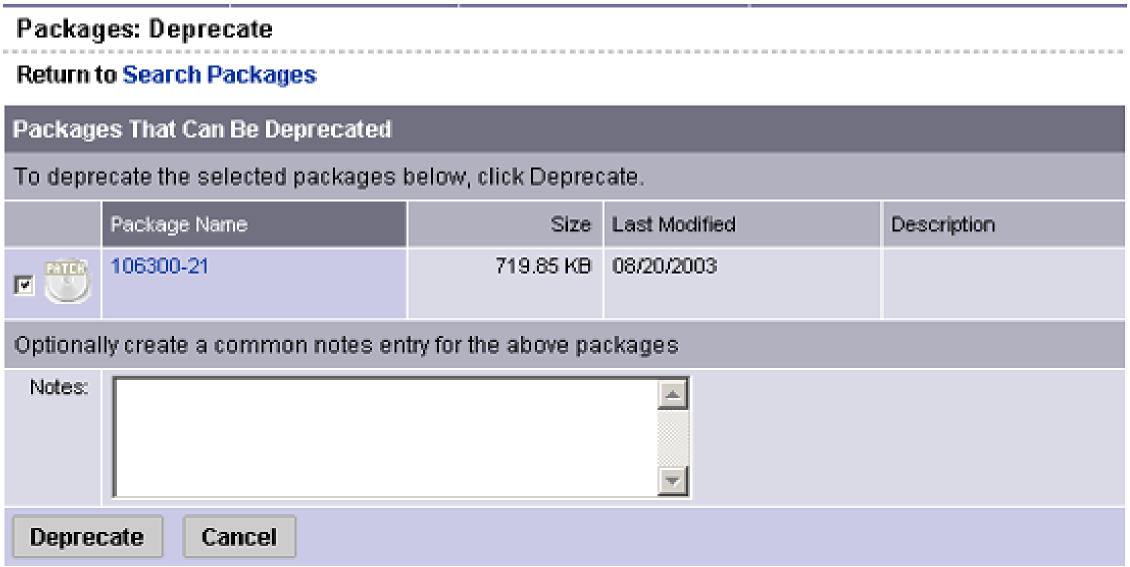
In most cases, a new package replaces the deprecated version. You can record this information in the Notes field for the package that you are deprecating.

You can also deprecate a package while you view the package properties. See “Editing Package Properties” on page 217 in this chapter for more information.

Perform the following steps to deprecate a package:

1. From the navigation panel, click Software ➤ Packages. The Packages: Browse Packages page appears.
2. Select the check boxes next to the packages that you want to deprecate.
3. Click the Deprecate button. The Packages: Deprecate page appears, as Figure 7-8 shows.

Figure 7-8: Packages: Deprecate Page



Packages: Deprecate

Return to Search Packages

Packages That Can Be Deprecated

To deprecate the selected packages below, click Deprecate.

	Package Name	Size	Last Modified	Description
☑ PATCH	106300-21	719.85 KB	08/20/2003	

Optionally create a common notes entry for the above packages

Notes:

4. To record the version of a new package that replaces the deprecated version, enter the information in the Notes field.
5. Click the Deprecate button.

Restrictions on Deprecating Packages

Deprecation is not allowed if the following conditions are true:

- The package is not attachable to nodes.
- The user does not have permission to access resources for that customer.
- The package is already deprecated.

Downloading a Package

You can download a package to your local computer so that you can check the installation of the package on a test or staging machine.

Package types that are not physical files – like APARs – cannot be downloaded so no download button appears for those file types.

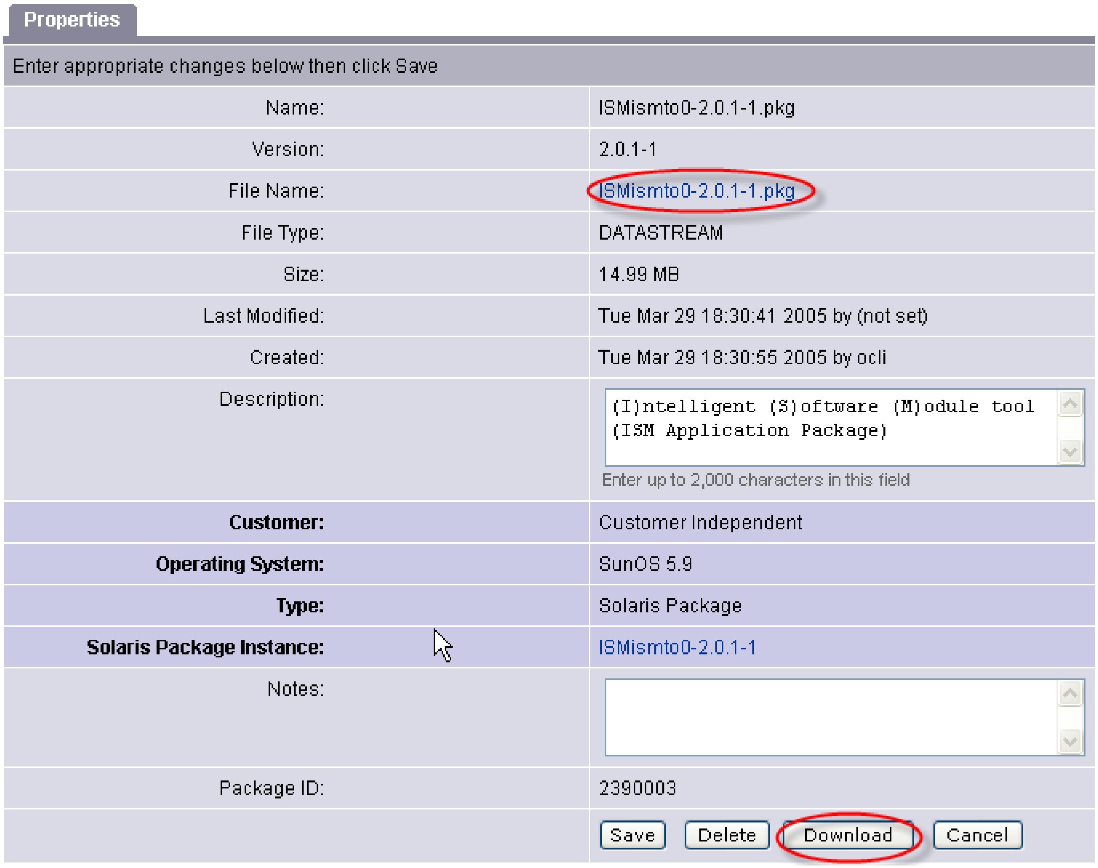
Perform the following steps to download a package:

1. Locate the package that you want to download. Locate the package by browsing (See “Displaying Packages” on page 206 in this chapter for more information) or by searching (See “Searching for Packages” on page 208 in this chapter for more information).

2. Click the package name link for the package that you want to download. The Packages: Edit Properties page appears. Click the Download button at the bottom of the page. OR

   In the File Name field, click on the link to download the package.

Figure 7-9: Downloading a Package



Enter appropriate changes below then click Save

Name:	ISMismto0-2.0.1-1.pkg
Version:	2.0.1-1
File Name:	ISMismto0-2.0.1-1.pkg
File Type:	DATASTREAM
Size:	14.99 MB
Last Modified:	Tue Mar 29 18:30:41 2005 by (not set)
Created:	Tue Mar 29 18:30:55 2005 by ocli
Description:	(I)ntelligent (S)oftware (M)odule tool (ISM Application Package) Enter up to 2,000 characters in this field
Customer:	Customer Independent
Operating System:	SunOS 5.9
Type:	Solaris Package
Solaris Package Instance:	ISMismto0-2.0.1-1
Notes:	
Package ID:	2390003

Chapter 8: OCLI 1.0 for Package Management

IN THIS CHAPTER

This chapter discusses the following topics:

- Opsware Command Line Interface Installation
- Software Repository OCLI
- Supported Operating Systems and Package Types

Opsware Command Line Interface Installation

To download the Opsware Command Line Interface packages for installation, you must have read permission to the Opsware customer. Contact your Opsware administrator to obtain the necessary access rights.

Before you use the Opsware Command Line Interface (OCLI), you must install the Opsware Agent and OCLI packages on the host from which you want to use the OCLI. See the *Opsware® SAS 5.2 User's Guide* for more information on installing an Opsware Agent.

Perform the following steps to install an OCLI package:

1 Download the package from the Opsware Command Center:

Search for the package OCLI. From the Search panel, enter `ocli` in the Search box, select the Packages option in the list, and click the Go button. The Packages: Search Packages page appears that displays all packages that match the search criteria. More than one page might result from the search. Use the navigation bar at the bottom of the page to move from page to page.

Each operating system and operating system version has different packages.

2. Click the package name for the OCLI that you want to download. The Packages: Edit Properties [*package name*] page appears.

3. Click the Download button to save the package locally.

4. Copy the OCLI package to each host on which you want to use the OCLI.

5. Perform the following steps, which vary by operating system:

   For Unix

   1. The file downloads as a non-executable file. Change the file mode to executable.
   2. Execute the package as root by entering the following command at the prompt:

      ```
      <package_name> -d <installation_directory>
      ```

Specifying the directory (-d `<installation_directory>)` in which to install the OCLI is optional. If you do not specify the installation directory, the OCLI is installed in the current directory.

   3. Include the file `login.csh` or `login.sh` in your environment, depending upon which shell you use.

      - For the shells csh, tcsh, and other variants, enter the following command at the prompt:

        ```
        source <installation_directory>/ocli/login.csh
        ```

      - For the shells sh, bash, ksh, and other variants, enter the following command at the command line:

        ```
        .<installation_directory>/ocli/login.sh
        ```

   4. Include `/opt/OPSW/bin` in your PATH.

      - For the shells csh, tcsh, and other variants, enter the following command at the prompt:

        ```
        setenv PATH /opt/OPSW/bin:${PATH}
        ```

- For the shells sh, bash, ksh, and other variants, enter the following command at the command line:

  ```
  export PATH=/opt/OPSW/bin:${PATH}
  ```

For Windows

1. Execute the package as Administrator.

   ```
   <package_name> -d <installation_directory>
   ```

2. Launch a command window and enter the following command at the prompt:

   ```
   set PATH=%PATH%;<installation.dir>\ocli\scripts
   ```

3. In the command window, enter the following command at the prompt:

   ```
   set PATH=%PATH%;%SYSTEMDRIVE%\Program
   Files\Loudcloud\lcpython15
   ```

Software Repository OCLI

This section provides information on the Software Repository OCLI and contains the following topics:

- Overview of Software Repository OCLI
- File Transfer Commands
- Syntax for the Commands

Overview of Software Repository OCLI

You can use the Opsware Command Center to manage packages in the Software Repository. See “Package Management” on page 187 in Chapter 7 for more information.

As a backup to access the Software Repository and for bulk uploads and downloads, you can use the OCLI.

You can only upload or download packages for the customer associated with the server from which you are running the OCLI. Contact your Opsware administrator to obtain the necessary access rights. If you must upload or download a package for a different customer, use the Opsware Command Center to change the customer association for the server. See the *Opsware® SAS 5.2 User's Guide* for more information about editing the properties of a server.

Servers *cannot* be associated with Customer Independent; therefore, if you need to upload a package associated with Customer Independent, you must upload it from a server associated with the Opsware customer. Associating a server with the Opsware customer can be a security issue; therefore, you should control the access to this server while it is associated with the Opsware customer.

The interface to each command is a CLI that begins with 'o' and has a prefix denoting the category of operation that it performs.

The commands and their associated interfaces are available on these operating systems that Opsware SAS supports: Solaris, Linux, AIX, HP-UX, Windows NT, Windows 2000, and Windows 2003.

All commands support standard POSIX-style command line options (single dash, single letter, such as -h) and GNU-style command line options (double dash, multiple letters, such as `--help`).

File Transfer Commands

Table 8-1: File Transfer Commands

COMMAND	DESCRIPTION
`oupload`	Upload a file to the Software Repository.
`odownload`	Download a file from the Software Repository.

Syntax for the Commands

```
oupload [options] filenames
```

The filename can contain a relative or absolute local file path.

```
odownload [options] filenames [localpath]
```

The *localpath* can contain a relative or absolute local file or directory path.

Using the OCLI to Access the Software Repository

Perform the following steps to use the OCLI to access the Software Repository:

1. After fully testing a package, upload the package to the Software Repository by entering the following command at the prompt:

   ```
   oupload --pkgtype <package_type> --customer <customer> --os
   <operating_system> <source_path>
   ```

If a value for an option contains spaces, you must enclose the value in quotation marks.

For RPM packages, always remember to upload the source files after uploading a package. Uploading the source files is important from a maintenance perspective because it allows users to modify packages at a later date.

2. After you upload the files, verify that they exist on the Software Repository by using the Search Panel function in the Opsware Command Center. Select package from the drop-down list, and use * as the name of the file.

After you upload a package, define the appropriate node in the Software Tree for the new package and attach the package to the node. See "Software Provisioning Setup" on page 247 in Chapter 10 for more information.

3. (Optional) To download a package from the Software Repository by using the OCLI, enter the following command at the prompt:

   ```
   odownload [options] <filename> <local_path>
   ```

   See "Options Common to All Commands" on page 233 in this chapter for information about a description of the options for the `odownload` command.

See “Unique Options for the oupload Command” on page 237 in this chapter for information about a description of the options for the `oupload` command.

Example: Using the OCLI

To upload `iPlanet_Web_Server-4.1sp19-LC~0.sparc64.rpm` for the customer Opsware and the operating system Solaris 5.8, enter the following command at the prompt:

```
oupload --pkgtype RPM --customer Opsware --os ”SunOS 5.8”
iPlanet_Web_Server-4.1sp19-LC~0.sparc64.rpm
```

If a value contains spaces, you must enclose the value in quotation marks.

Options Common to All Commands

Table 8-2: Options Common to all Commands

ARGUMENTS	VALUES	DESCRIPTION

`--customer <value>`
`(-C=X)`
	String (customer name, wildcards accepted) or integer (customer ID)	Specifies the customer of the file. Specifying this option is required unless you are using `--patchtype` in `oupload`.
		When you upload an AIX LPP file, or an HP-UX Depot that contains patches, it is associated with “Customer Independent” regardless of the customer you enter by using the `-c` option.
		When you upload an AIX Maintenance Level set of LPPs, you must associate them with “Customer Independent” so that all base filesets and update filesets contained in it are associated with the same customer.

Table 8-2: Options Common to all Commands

ARGUMENTS	VALUES	DESCRIPTION

`--feedback`
`(-Q)`
	N/A	Displays feedback while the command runs. By default, this option is enabled.
		Cannot specify this option with `–q`

`--fr` *`<value>`*
`(-f=X)`
	• Alphanumeric
	• Period
	• Hyphen
	• Default = theword
		Specifies the hostname or IP address of the Software Repository

`--frport` *`<port>`*
`(-F=X)`
	Integer
	Default = 1003
		Specifies the port of the Software Repository

`--fullhelp`
`(-H)`
	N/A	Displays full help information
		Cannot specify this option with `-h` or `–V`

`--help`
`(-h)`
	N/A	Displays abbreviated help information
		Cannot specify this option with `-H` or `–V`

`--nofeedback`
`(-q)`
	N/A	Does not display feedback while the command runs
		Cannot specify this option with `–Q`

Table 8-2: Options Common to all Commands

ARGUMENTS	VALUES	DESCRIPTION

`--os <type>`
`(-O=X)`
	String (OS name, wildcards accepted) The following are the allowable values:
	See "Allowable Strings and Integer Values for -os Option" on page 236 in this chapter for more information
		Specifies the operating system of the package
		Specifying this option is required.
		If a value has a space in the name, enclose the entire name in quotes.
		For Fujitsu Solaris 2.8, use the value for Solaris 8. For Fujitsu Solaris 2.9, use the value for Solaris 9.

`--timeout <value>`
`(-z=X)`
	Integer
	Default = 60
		Sets the timeout to the server in seconds

`--truthgw <value>`
`(-g=X)`
	• Alphanumeric
	• Period
	• Hyphen
	• Default = spin
		Specifies the hostname or IP address of the Data Access Engine

`--truthgwport <port>`
`(-G=X)`
	Integer
	Default = 1004
		Specifies the port of the Data Access Engine

`--verbose`
`(-v)`
	N/A	Displays debug information

`--version`
`(-V)`
	N/A	Displays version information for the OCLI
		Cannot specify this option with `-h` or `–H`.

Allowable Strings and Integer Values of -os Option

Table 8-3: Allowable Strings and Integer Values for -os Option

STRING NAME (OS NAME)	INTEGER VALUE (ID)
AIX 4.3	870007
AIX 5.1	10001
AIX 5.2	260007
AIX 5.3	40007
HP-UX 10.20	230007
HP-UX 11.00	1070007
HP-UX 11.11	1080007
OS Independent	1
Red Hat Enterprise Linux AS 2.1	960007
Red Hat Enterprise Linux AS 3.0	430007
Red Hat Enterprise Linux ES 2.1	10730013
Red Hat Enterprise Linux ES 3.0	10720013
Red Hat Enterprise Linux WS 3.0	270022
Red Hat Enterprise Linux 6.2	140000
Red Hat Enterprise Linux 7.1	210022
Red Hat Enterprise Linux 7.2	950007
Red Hat Enterprise Linux 7.3	410007
Red Hat Enterprise Linux 8.0	420007
SUSE Linux Standard Server 8.0	20007
SUSE Linux Enterprise Server 8.0	10030
SUSE Linux Enterprise Server 9.0	20032
SunOS 5.6	130000
SunOS 5.7	90000
SunOS 5.8	150001
SunOS 5.9	920007

Table 8-3: Allowable Strings and Integer Values for -os Option

STRING NAME (OS NAME)	INTEGER VALUE (ID)
Windows 2000	120000
Windows 2003	10007
Windows NT 4.0	8000

Unique Options for the oupload Command

The Opsware Command Line Interface (OCLI) includes arguments which allow you to specify an encoding scheme when uploading and downloading packages and for the customer display name

You only need to enter these arguments when you want to override the default settings in the LANG environment variable in your shell.

Table 8-4: Unique Options for the oupload Command

ARGUMENTS	VALUES	DESCRIPTION

`--patchtype <type>`
`(-a=X)`
	• AIX LPP
	• HP-UX Depot
	• Windows Hotfix
	• Windows Service Pack
	• Solaris Patch
	• Solaris Patch Cluster
		Cannot specify this option with `-C`.

Table 8-4: Unique Options for the oupload Command

ARGUMENTS	VALUES	DESCRIPTION

`--pkgtype <type>`
`(-t=X)`
	• AIX LPP
	• HP-UX Depot
	• RPM
	• Windows Hotfix
	• Windows MSI
	• Windows Service Pack
	• Solaris Package
	• Solaris Patch
	• Solaris Patch Cluster
	• Microsoft Patch Database
	• OS Provisioning Install Hooks
	• Windows Zip File
		Specifies the type of file.
		Specifying either this option or the `-patchtype` option is required.
		Wildcards are accepted.
		The OCLI does *not* support uploading response files for the Solaris Package package type. Use Opsware Command Center to associate a response file with a Solaris Package. See "Editing Package Properties" on page 217 in Chapter 7 for more information.
		If a value contains spaces, you must enclose the value in quotation marks.

--filename-encoding (-e)	String	Specifies the character set of the file name When specifying non-ASCII characters in the value for the --customer argument, include the -e argument on the command line to tell Opsware SAS which character set to use when communicating with the Model Repository database.

Table 8-4: Unique Options for the oupload Command

ARGUMENTS	VALUES	DESCRIPTION
--metainfo-encoding (-E)	String	Specifies the character set of the meta-information in the package

Unique Options for the odownload Command

You only need to enter this argument when you want to override the default settings in the LANG environment variable in your shell.

The following table shows the new arguments for the `odownload` command.

Table 8-5: New Arguments for the odownload Command

ARGUMENT	VALUE	DESCRIPTION
--filename-encoding (-e)	String	Specifies the character set encoding in which to save the file name

The following table includes the values that must be supplied interactively based on the package type.

Table 8-6: Values for Package Types

PACKAGE TYPE	OPTIONS	DATA TYPE
Windows Hotfix	N/A	N/A
Windows MSI	Product version Product name	Free form text
Windows OS Service Pack	Service pack level	Free form text
AIX LPP	N/A	N/A
HP-UX Depot	N/A	N/A
RPM	N/A	N/A
Solaris Package	N/A	N/A
Solaris Patch	N/A	N/A
Solaris Patch Cluster	N/A	N/A
Unknown	N/A	N/A
Microsoft Patch Database	N/A	N/A (Can only be uploaded for Windows 2000)
OS Provisioning Install Hooks	N/A	N/A
Windows Zip File	N/A	N/A
Windows Utility	N/A	N/A (Can only be uploaded for Windows 2000)

Supported Operating Systems and Package Types

Each operating system that Opsware SAS supports has a list of package types that you can upload. Opsware SAS supports these package types on the supported operating systems, as the following table shows.*

Table 8-1: Supported Operating Systems and Package Types

OPERATING SYSTEM	PACKAGE TYPE	FILE FORMATS	ADDITIONAL METADATA*
AIX	LPP (contains an update fileset or base filesets)	.bff	N/A
	RPM	.rpm	N/A
HP-UX	Depot (contains products and filesets)	.tar	N/A
Linux	RPM	.rpm	N/A
Solaris	Patch	.jar, .tar, tar.gz, .tar.Z, t.gz, .zip	N/A
	Patch Cluster (contains patches)	.tar, .tar.gz, tar.Z, .t.gz, .zip	N/A
	Solaris package (contains package instances)	Datastream File	N/A
	RPM	.rpm	N/A

Table 8-1: Supported Operating Systems and Package Types

OPERATING SYSTEM	PACKAGE TYPE	FILE FORMATS	ADDITIONAL METADATA*
Windows	Hotfix	.exe	N/A
	Security Patch	.exe	N/A
	MSI	.msi	Product version and name
	OS Service Pack	.exe	Service Pack Level
	Windows Utility (Microsoft Security Baseline Analyzer and qchain)	.exe	N/A
	Microsoft Patch Database (contains a description of available patches) See “About the Microsoft Patch Database” on page 412 in Chapter 8 for more information.	.xml, .cab	N/A
	ZIP	.zip	N/A
OS Independent	Unknown	All	N/A

For certain package types, the Opsware Command Center requires that you provide additional metadata for the package.

Chapter 9: Software Repository Replicator Setup

IN THIS CHAPTER

After you install an Opsware core in multimaster mode, you can set up replication for the Software Repository in a facility.

This chapter discusses the following topics:

- Overview of the Software Repository Replicator
- Prerequisites for Using the Software Repository Replicator
- Software Repository Replicator Configuration

Overview of the 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 allows you to have redundant copies of Software Repositories and thereby helps to ensure that all packages remain available even when a Software Repository goes offline.

Prerequisites for Using the Software Repository Replicator

Before you set up the Software Repository Replicator, you must meet the following prerequisites:

- SSH must be installed on the source and target Software Repositories.
- Port 22 must be open on the firewalls.

- Passwordless SSH as root must be enabled between the source and target repositories.

Software Repository Replicator Configuration

By default, the Opsware Installer installs the software you need to set up Software Repository replication when you install the multimaster Software Repository.

From the source core, use the `replicator.conf` file found in the `/cust/word/etc/` directory to configure the Software Repository Replicator.

To set up Software Repository replication, you do *not* need to modify the `replicator.conf` files in the target cores. However, you must specify to replicate the directory `/cust/word/etc/` to all the target cores. You specify which target cores to replicate to by entering them in the host chain section of the `replicator.conf` file. When you specify replication to these target cores, the `replicator.conf` file will propagate to the Software Repositories in the target cores.

See the bullet about defining host chains on page 245. See "Sample Software Repository Replicator Configuration" on page 246 in this chapter for information about an example of how to specify target cores in a host chain.

In this file, you must specify the following settings:

- The values for `User`, `Timestampdir`, and `SSH_PATH`.

  The Software Repository Replicator keeps timestamps of when it runs.

- For each directory that you want to replicate, specify the Directory or WordDirectory tag.

  Before you set up replication for the Software Repository, you need to determine which directories to replicate. This guide does not document the entire file system directory hierarchy for the host running the Software Repository.

  To determine which directories you should consider replicating (and the configuration to accomplish this), contact your Opsware, Inc. Support Representative for assistance making this determination.

  The Software Repository Replicator parses the Directory tags, and these are ignored by the Software Repository. Therefore, you can use the Directory tag to replicate files that are not served by the Software Repository. WordDirectory tags are parsed by both the Package Replicator and the Software Repository.

You should specify these tags for each directory you want to replicate because the Software Repository Replicator is not the only process that parses the `replicator.conf` file. Some of the other processes that parse the `replicator.conf` file only use WordDirectory as a backup repository and ignore entries labeled “Directory.”

The directory `/cust/word/mmword_local` is a symlink; therefore, you need to replicate its target `/cust/word/<`*`facility_name`*`>`.

Do *not* replicate the directories for `mmword_cache` and `mmword_local`.

The Software Repository should ignore directories that are not actual software repositories while serving files (for example, files should not be served from the

`/cust/word/etc/` directory.)

- Specify the replication rate in seconds.

Define host chains. Make sure that the host names you specify are the actual host names (that is, the same that the hostname command returns).

For example, `hostA hostB hostC` means that a directory will be replicated from hostA to hostB to hostC.

For example `hostA hostB`, `hostA hostC` means that a directory will be replicated from hostA to hostB and from hostA to hostC.

In these examples, if you want the packages on each Software Repository host backed up, all the hosts have to be in the same multimaster mesh.

Verify that you can use passwordless SSH to connect from the source host to the destination host as it is specified for each host chain in the `replicator.conf` file (that is, if you specify FQDN, try to connect with SSH with FQDN even if `host.subdomain` resolves to the correct location.)

After you configure the Software Repository Replicator, you must re-start the replicator so that it will automatically re-read its configuration file. At each destination core, wait the time period you specified in the `replicator.conf` file before you re-start the replicator.

To re-start the replicator, enter the following command on the server running the Software Repository component:

```
/etc/init.d/replicator [start/stop]
```

Sample Software Repository Replicator Configuration

```
User: root
Timestampdir: /var/lc/replicator
SSH_PATH: /lc/bin/ssh
Directory: 60 /cust/word/etc
Chain: theword01.subdomain1.domain.com
     theword01.subdomain2.domain.com
Chain: theword01.subdomain1.domain.com
     theword01.subdomain3.domain.com
WordDirectory: 60 /cust/word/facility1
Chain: theword01.subdomain1.domain.com
     theword01.subdomain2.domain.com
WordDirectory: 60 /cust/word/facility2
Chain: theword01.subdomain2.domain.com
     theword01.subdomain3.domain.com
WordDirectory: 60 /cust/word/facility3
Chain: theword01.subdomain3.domain.com
theword01.subdomain1.domain.com
```

Chapter 10: Software Provisioning Setup

IN THIS CHAPTER

This chapter discusses how to prepare to provision applications by setting up nodes in the Software Tree and creating templates. This chapter discusses the following topics:

- Software Tree
- Managing Nodes on the Software Tree
- Software Attached to Nodes
- Custom Attributes Set for the Environment
- Templates and Folders
- Working with Folders and Templates

A user must have specific permissions to manage applications that use the Opsware Command Center. Contact your Opsware administrator to obtain the necessary access rights.

This chapter assumes that users have already packaged software applications and uploaded the packages to the Software Repository. See “Uploading a Package” on page 211 in Chapter 7 for information about how to upload packages to the Software Repository.

See *Planning Deployments for Opsware® SAS 5.2* for more information about Software Tree best practices.

Software Tree

This section provides information on the Software Tree within Opsware SAS and contains the following topics:

- Overview of Software Tree

- Example of a Software Tree
- Guidelines for Setting Up the Software Tree
- How to Use the Software Tree
- Understanding How Software Is Reconciled onto Servers
- When to Reconcile

Overview of Software Tree

Many IT organizations define policies for creating systems in their operational environment by setting standards for configuration and processes. Defining policies and standardizing repeated processes minimizes custom work and creates efficiency and reliability because the same policies are used throughout the installation.

Opsware technology enables IT organizations to implement their policies by using Opsware's model-based approach to manage an operational environment. The model can:

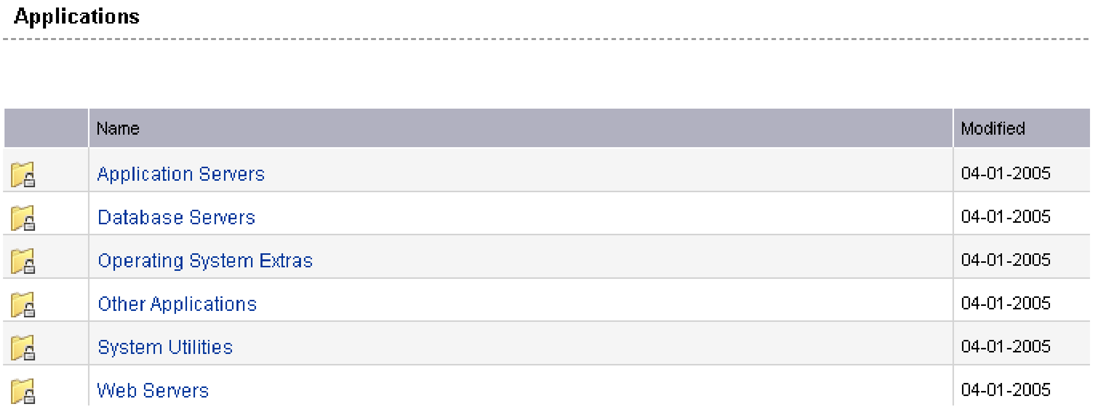
- Encapsulate policies for creating systems in an operational environment
- Contain a comprehensive picture of an operational environment

See the *Opsware® SAS 5.2 User's Guide* for more information.

The Opsware Command Center visualizes the model as a tree called the *Software Tree*. The Software Tree is made up of nodes and subnodes, which model the interrelationships and dependencies among the software and customer accounts in an operational environment. Users navigate the Software Tree to perform specific operations.

The top level of the Software Tree for Applications has six default main categories. These categories display on the Applications page as Figure 10-1 shows. You can access the Applications page from the navigation panel by clicking Software ➤ Applications.

Figure 10-1: Top Level of Applications Page



Applications

	Name	Modified
📁	Application Servers	04-01-2005
📁	Database Servers	04-01-2005
📁	Operating System Extras	04-01-2005
📁	Other Applications	04-01-2005
📁	System Utilities	04-01-2005
📁	Web Servers	04-01-2005

These six default main categories are defined as follows:

- Application Servers, such as WebLogic, connect the database information with the client program, such as the Web browser.
- Database Servers, such as Oracle or Microsoft SQL Server, contain and manage the database.
- OS Extras, which are optional, contain applications that need to be installed directly after an operating system, for example, VCS or special utility software.
- Other Applications is a catch-all category for software that does not fit into the other categories. Try to add software to one of the other categories before you add a node in this category.
- System Utilities are such as PC Anywhere, JDK, Open SSL, or Winzip.
- Web Servers, such as Apache, Microsoft Internet Information Server, or iPlanet are server processes running at a Web site that deliver Web pages in response to browser requests.

No additional categories can be added, and categories cannot be deleted or modified.

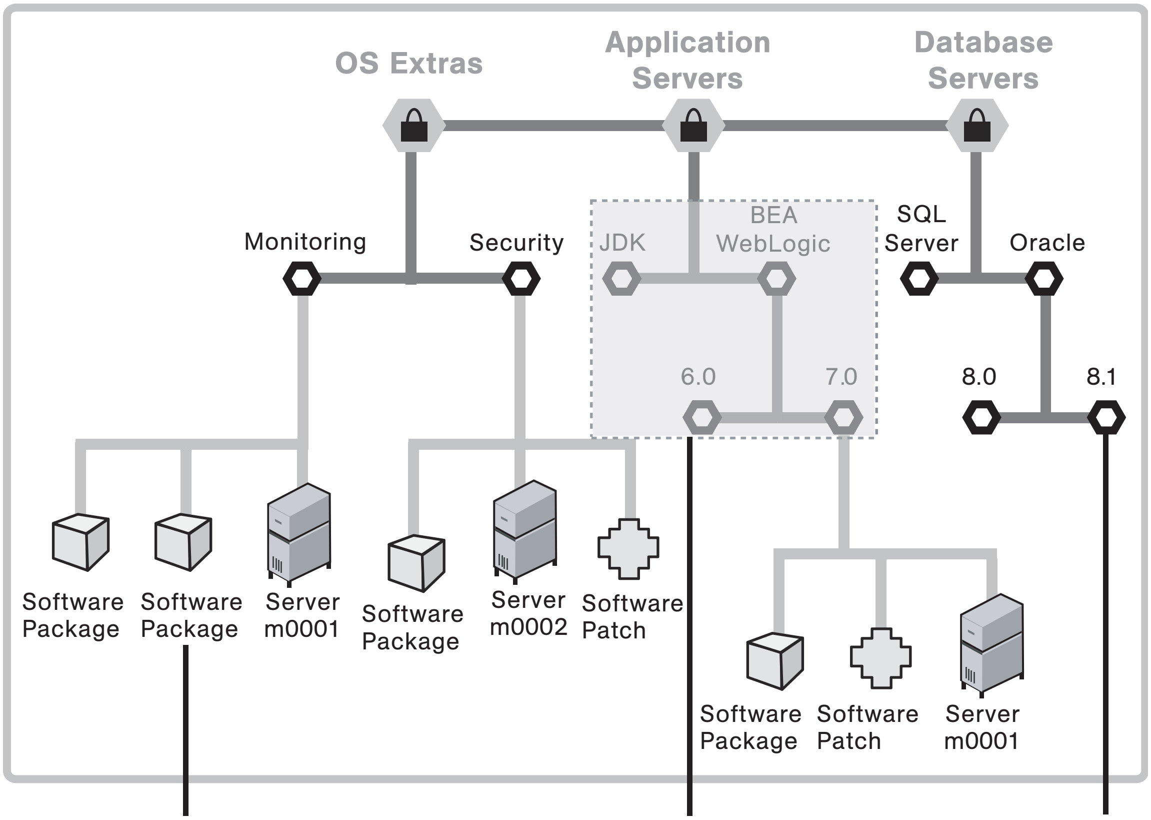
The Software Tree has the following characteristics:

- Each point in the Software Tree is called a *node*.
- A node inherits properties or software from the nodes above it.
- Software or a server might be attached to a node depending on its location in the Software Tree. See “Software Attached to Nodes” on page 271 in this chapter for more information.
- Attaching a server to a node determines what software is installed on that server and how it is configured.
- Users can add nodes and subnodes within each category.
- The node information at the top of the Software Tree is more general, and as you travel farther down the tree, each successive subnode contains more details and specific information that relates to the node above it.

Example of a Software Tree

Figure 10-2 shows how three categories and the nodes within them might be defined at a site.

Figure 10-2: Example of How Nodes and Subnodes Are Defined Within the Software Tree



A package containing an application; packages can also contain patches

A template, which is a collection of nodes to which packages are added

A node in the Software Tree

In the figure, servers and software are attached to the Software Tree in the following locations:

- Server hostname m0001 is attached to the Application Servers BEA WebLogic 5.8 node and the Monitoring node.
- Server hostname m0002 is attached to the Application Servers BEA WebLogic 5.8 node and the Security node.

Users can attach servers to multiple nodes within the same category, as well as nodes in different categories.

Guidelines for Setting Up the Software Tree

When you build the model of an operational environment, the Software Tree should:

- Describe all facets of the managed environment.
- Be customizable.
- Be extensible – when something new is learned, the model is updated.

To keep the information consistent, Opsware Inc. recommends that users follow this structure when they create new nodes within a category:

Category Name ➤ Product Name ➤ Operating System ➤ Product Version ➤ Node Version

For example:

Application Servers ➤ Vignette ➤ Solaris 7➤ v1

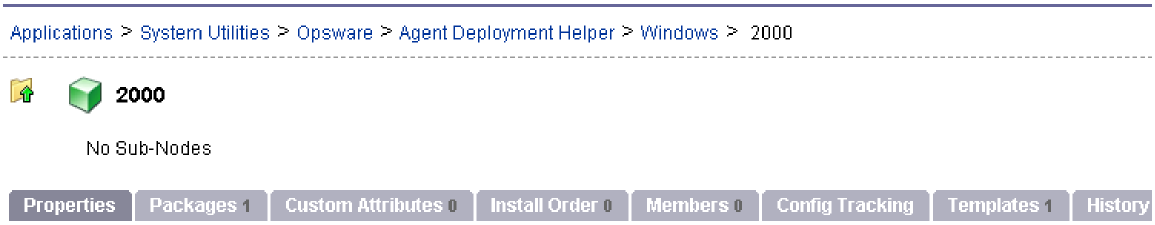
- Some nodes do not have software or attributes attached to them because either they inherit the software or attributes from their parent nodes, or they are used for organizational purposes.
- In most cases, you attach servers to nodes at the end of the Software Tree path because servers need to be attached to nodes at the point where the proper operating systems, software, versions, and so forth that belong on that particular server have been identified.
- Opsware Inc. recommends organizing your Software Tree with the operating system preceding the product version because all software versions might not be available for each operating system.
- The best general rule is to keep the structure consistent, organized, and simple.

See *Planning Deployments for Opsware® SAS 5.2* for more information about Software Tree best practices.

How to Use the Software Tree

Figure 10-3 demonstrates the node hierarchy as it goes from the general to the specific–System Utilities is the category, Opsware is a node in that category, Agent Deployment Helper is a subnode of Opsware, Windows is a subnode of Agent Deployment Helper, and 2000 is a subnode of Windows. The tabs used for all functions in Applications are also shown.

Figure 10-3: Application Hierarchy



When you navigate through the Software Tree, you can perform actions on a node by using the tabs. Table 10-1 gives descriptions of the available tabs.

Table 10-1: Tabs Available for Applications

TAB PAGE	DESCRIPTION
Properties	View general information about the node, including restrictions for using the node (such as whether servers can be attached, and the operating systems and customers of the packages and servers that can be attached).
Packages	Manage all software associated with a node, including adding and deleting packages, changing the order of installation, and overriding software attachments that would be inherited from a parent node.
Custom Attributes	Set custom attributes for servers that apply to all servers attached to a node. These custom attributes include setting miscellaneous parameters and named data values. Users can write scripts that use these parameters and data values when performing a variety of functions, including network and server configuration, notifications, and CRON script configuration.
Install Order	Create and delete dependencies that specify the order of software installation on servers.

Table 10-1: Tabs Available for Applications

TAB PAGE	DESCRIPTION
Members	Manage all servers and server groups associated with a node. Manage servers by reconciling servers between nodes, installing applications, installing patches, and so forth. See the *Opsware® SAS 5.2 User's Guide* for information about how to use these functions.
Config Tracking	View and add entries in the configuration tracking policy for a node. See "Configuration Tracking Setup" on page 387 in Chapter 13 for more information.
Templates	Lists the templates attached to a node.
History	View the audit trail for changes made to a node. View events such as when servers were attached to nodes, subordinate nodes were added, or customers or operating systems were associated with nodes.

Understanding How Software Is Reconciled onto Servers

A user installs software on a server by using the packages that are stored in the Software Repository. In the Opsware Command Center, the user adds a package to a node, and then attaches a server to that node. When the user reconciles the server, Opsware SAS installs the software on the server.

See *Opsware® SAS 5.2 User's Guide* for more information about how to reconcile.

When your node hierarchy is completely defined in the Software Tree, and software and servers are attached, you are ready to perform the reconcile function to install the software on those servers. Opsware SAS retrieves the information about the software currently installed on the server, compares it to the list of software about to be installed, and determines any differences. The reconcile function installs the specified software and possibly also removes software, depending upon the type of reconcile being performed. Before you install the software, the Opsware Command Center displays a preview of the actions about to be performed so that you can make any necessary changes before you proceed.

When to Reconcile

Whenever you make a change to a node that deals with attached software or with custom attributes, you have to reconcile any servers that are attached to that node in order for those changes to be applied. Whenever an application is installed or uninstalled using the Software Install or Software Uninstall Wizard, the Wizard automatically starts a reconcile.

Managing Nodes on the Software Tree

This section provides information on how to manage nodes on the Software Tree and contains the following topics:

- Overview of Software Provisioning Setup Tasks
- Adding a Node to the Software Tree
- Editing a Node in the Software Tree
- Deleting a Node in the Software Tree
- Copying a Node in the Software Tree
- Moving a Node in the Software Tree
- Managing a Node’s Configuration Tracking Policy
- Viewing Node History

Overview of Software Provisioning Setup Tasks

It is important to manage the nodes on the Software Tree by adding them appropriately and attaching packages appropriately in order to make sure that your servers are properly provisioned with applications.

Users perform the following tasks when setting up and managing the Software Tree and templates:

- Create, edit, and delete nodes.
- Add to, remove from, and define the order of software packages on nodes.
- View and manage software inherited from another node.
- Add, remove, and edit custom attributes.

- Define package installation order so that packages are installed on servers in a specific order.
- Create and edit a node's configuration tracking policies. See "Node-Based Tracking Policies" on page 398 in Chapter 13 for more information.
- View the changes to nodes.
- Create, edit, and delete templates.

Adding a Node to the Software Tree

Within each of the categories, users can create subordinate nodes that extend a node, inheriting software packages or other attributes from their parent nodes and adding new software, updates, or other information.

Reasons for Adding a Node

Normally, you do not modify an existing node that has attached servers. The next time a user reconciles the servers, the users inadvertently upgrade the packages to the latest version or remove packages from the servers. So, if you need to apply a change to only a subset of servers attached to a node, consider creating a subordinate node. If you want to add a later version of a package, consider creating a sibling node with the new version number and moving the servers that you plan to reconcile to it. See the *Opsware® SAS 5.2 User's Guide* for more information about reconcile.

For example, you might want to keep package version 1 separate from version 1.1 because you want to upgrade only one customer to version 1.1. In this example, nine servers for three different customers are attached to the node for version 1. You do not want to upgrade all the customers' servers. Create a new node for version 1.1 and move the three servers that you want to upgrade to the version 1.1 node.

Restrictions When Adding Nodes

Nodes can be added at any level on the Software Tree by users with the proper permissions. The only restriction is that no nodes can be added at the category level at the top of the tree.

How to Add a Node

Perform the following steps to add a node:

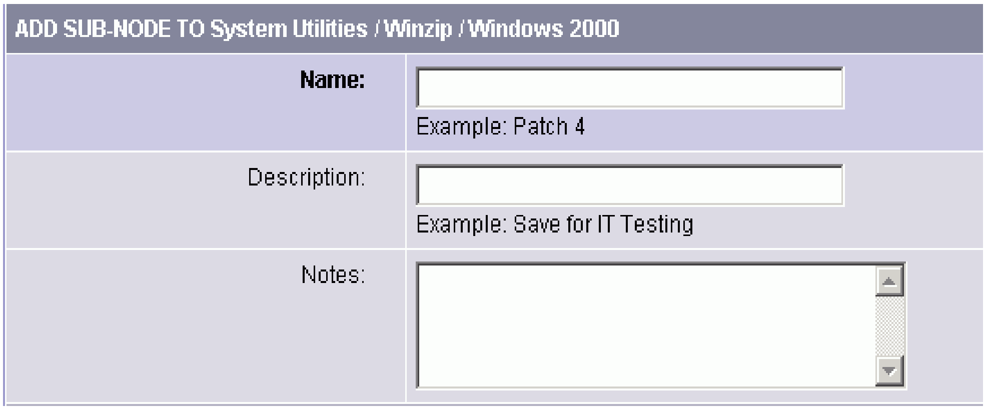
1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Click the appropriate category.

3 If you are adding a new node to the Software Tree, click the Add button.

4 If you are adding a node to an existing branch on the Software Tree, first navigate to the point in the Software Tree where you want to add a node (for example, System Utilities ➤ Winzip ➤ Windows 2000) and then click the Add button.

The Add Sub-Node form appears, as Figure 10-4 shows. (If a lot of nodes display, you might need to scroll down to see the form.)

Figure 10-4: Adding a Sub-Node to an Existing Node or Category



ADD SUB-NODE TO System Utilities / Winzip / Windows 2000

Name:	Example: Patch 4
Description:	Example: Save for IT Testing
Notes:	

5 Complete the entries that define the node:

- Enter a name (required).

  The name is limited to 255 characters; names for nodes under the same parent node must be unique. Names are used in the display of the node navigation path, for example:

  Application Servers ➤ WebLogic ➤ Solaris 6

- (Optional) In the Description text box, enter a one-line description (up to 500 characters) and indicate why the node was created and what is special about it.

- (Optional) In the Notes text box, enter any other more detailed notes (up to 4000 characters) that you want others to know about the node.

The bottom section of the page shows information about what attributes the new node inherits from its parent, as well as what customers and operating systems the user can edit after creating the node.

6 Click the Save button at the bottom of the page. The Edit Attributes form appears.

7 Follow the instructions in the How to Edit a Node section in this chapter to complete this form.

In general, the most common attributes that need to be changed after you add a new node are Allow Servers, Change Customer, and Change Operating Systems.

Editing a Node in the Software Tree

After you create a node, you might need to make changes to the properties of the node instead of deleting it and creating a new node.

Reasons for Editing a Node

You can edit nodes to change the following properties:

- The name of the node in order to be consistent with your company's naming structure
- The description or notes about the node to clarify its function and purpose
- The Locked attribute to limit, or to remove limits on, access to the node
- The Allow Servers attribute that allows or disallows servers to be assigned to the node
- The Customer and Operating System attributes that define what software and templates can be attached

Restrictions When Editing Nodes

You cannot edit nodes in the following cases:

- The node is a category – Application Servers, Database Servers, OS Extras, Other Applications, System Utilities, or Web Servers – that appears on the top-level Applications page.
- The node is locked and you do not have the correct permissions to edit locked nodes for that category.
- The node is reserved (system - level attribute; user cannot use or modify).
- The node is derived (system -l evel attribute; user cannot use or modify).
- In a multiple facility environment, the node's data in one Model Repository conflicts with the data of the same node in another Model Repository.
- You do not have the correct read/write permissions for the customer of that node.

Each software package and each node has customer and operating system attributes associated with it that must match the package that is uploaded to the Software Repository. These attributes must match in order for the software to attach to a node. For example, software with a Solaris operating system (Sun Solaris node) cannot be attached to a node associated with a Linux operating system.

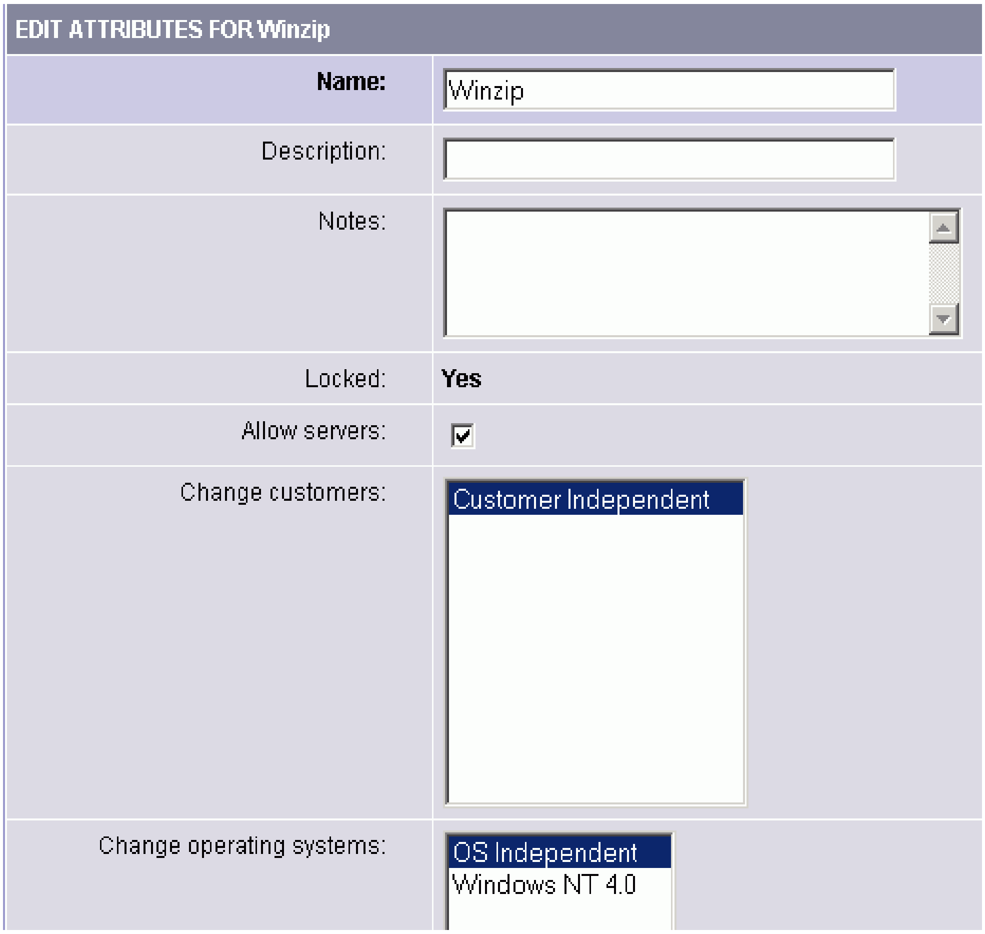
How to Edit a Node

Perform the following steps to edit a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the point in the node hierarchy where you want to edit a node (for example, System Utilities ➤ Winzip ➤ Windows 2000).

3 Click the Edit button. The Edit Attributes for [*node*] page appears, as Figure 10-5 shows.

Figure 10-5: Edit Attributes Page



EDIT ATTRIBUTES FOR Winzip

Name:	Winzip
Description:	
Notes:	
Locked:	**Yes**
Allow servers:	☑
Change customers:	Customer Independent
Change operating systems:	OS Independent Windows NT 4.0

4 Table 10-2 shows the fields that you can edit to update the node. Click the Save button when you are done.

Table 10-2: Field Data to Update for the Node

FIELD	DESCRIPTION
Name	Name, limited to 225 characters, that is used in the display of the node navigation path. For example: Application Servers ➤ WebLogic ➤ Soalris 8 Constraint: Names for nodes under the same parent node must be unique.
Description	One-line description that indicates why the node was created and what is special about it. Limited to 500 characters.
Notes	More detailed information that you want others to know about the node. Limited to 4,000 characters.
Locked	Locked nodes indicate that the node can only be edited by users with Opsware Locking Permissions for that category. If the user has the correct permission, the user is able to edit the attributes of the node, add and remove software, and add and remove custom attributes. Constraints: • Only privileged users–those with Opsware Locking Permissions–can lock and unlock nodes. • Nodes cannot be locked if the parent node is not locked. • Nodes cannot be unlocked if one or more subnodes are locked.
Allow Servers	Whether a server can be assigned to this node. If this option is selected, users have the node listed as an option in the Install Applications Wizard, the Server Assign dialog box, and the Server Reassign dialog box when managing servers (Manage Servers, My Servers, Server Search, and the Node Server tab). In addition, only nodes with this attribute selected can be assigned to templates. Constraint: Must be checked if servers are already assigned to the node or templates are assigned to the node.

Table 10-2: Field Data to Update for the Node

FIELD	DESCRIPTION
Change Customers	The customer that the node is associated with. This attribute determines who can view and edit the node (with the appropriate Opsware customer permissions), what software and servers can be attached, and what templates this node can be assigned to. Each node can only have one customer associated with it. Only customers that are valid for the node display. Sometimes, only the current customer is on the list, meaning that it cannot be changed. The list of customers that displays in the selection box varies. Only valid choices display. The following conditions affect what displays in the list: • If there are subnodes and what customers are associated with those nodes • If packages are attached and what customers are associated with those packages • If servers are attached to the node • Templates that the node is added to • What the parent node's customer is

Table 10-2: Field Data to Update for the Node

FIELD	DESCRIPTION
Change Operating Systems	Specifies the operating systems that the node is associated with. This attribute determines what software and servers can be attached and what templates this node can be assigned to. Each node can only have one operating system associated with it. Only operating systems that are valid for the node display. Sometimes only the current operating system is on the list, meaning that it cannot be changed. Nodes with the operating system OS Independent cannot have software attached. The list of operating systems that display in the selection box vary. Only valid choices display. The following conditions affect what the list displays: • If there are subnodes and what operating systems are associated with those nodes • If packages are attached and what operating systems are associated with those packages • If servers are attached to the node • Templates that the node is added to • What the parent node's operating system is

Deleting a Node in the Software Tree

You should only delete nodes if you no longer need to retain that intellectual property. All history, knowledge of that software in the model, custom attributes, and configuration tracking policies are removed when you delete a node. You cannot undo a deleted node.

Reasons for Deleting a Node

You might want to delete a node after you create it to test a new software installation. To keep the display of your node hierarchy well-organized, delete nodes that are no longer needed and whose information is no longer needed.

Restrictions When Deleting Nodes

You cannot delete a node when the node:

- Has servers attached
- Contains subordinate nodes

- Is a category (a top-level node)
- Belongs to a template
- Is locked (you must have special permission to delete these nodes)
- Is reserved (system level attribute; user cannot use or modify)
- Is derived (system level attribute; user cannot use or modify)
- The node's data in one Model Repository conflicts with the data of the same node in another Model Repository (multiple facility environment)

How to Delete a Node

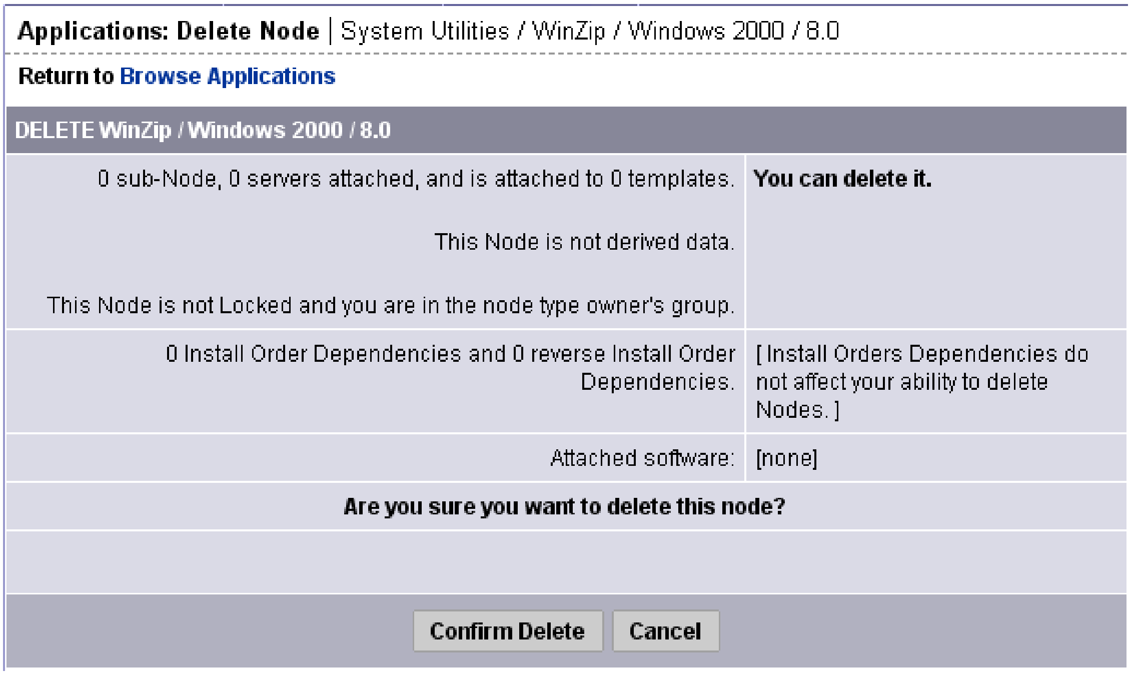
Perform the following steps to delete a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the node that you want to delete (for example, System Utilities ➤ Winzip ➤ Windows 2000).
3. Click the Delete button.

The Delete button does not appear if one or more of the above restrictions is true.

The Opsware Command Center displays a page that shows how many servers, subordinate nodes, and templates the node has. The number should be zero for all in order to delete the node. See Figure 10-6.

Figure 10-6: Applications: Delete Node Page



Applications: Delete Node | System Utilities / WinZip / Windows 2000 / 8.0

Return to Browse Applications

DELETE WinZip / Windows 2000 / 8.0	
0 sub-Node, 0 servers attached, and is attached to 0 templates. This Node is not derived data. This Node is not Locked and you are in the node type owner's group.	**You can delete it.**
0 Install Order Dependencies and 0 reverse Install Order Dependencies.	[Install Orders Dependencies do not affect your ability to delete Nodes.]
Attached software:	[none]

Are you sure you want to delete this node?

The display confirms how many software packages and installation order dependencies are associated with the node. The presence of software does not prevent a user from deleting a node.

You are prompted to confirm the deletion.

4 To delete the node, click the Confirm Delete button.

The Opsware Command Center returns you to the Properties page for the parent node.

Copying a Node in the Software Tree

The copy function is a convenient way to duplicate information that is contained in an existing node without having to enter the information all over again.

Reasons for Copying a Node

Use this function when you want to copy the structure and attributes from one node to a new node at the same level in the Software Tree.

Restrictions When Copying Nodes

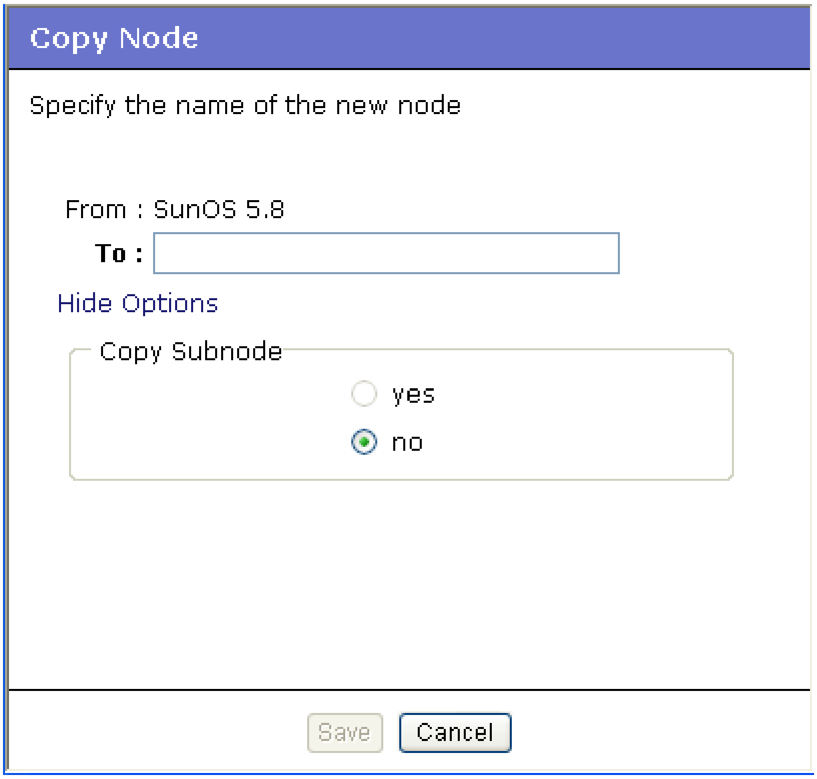
You can copy a node at any level, except the top-level categories.

How to Copy a Node

Perform the following steps to copy a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the node that you want to copy (for example, Application Servers ➤ WebLogic ➤ Solaris 8).
3. Click the Copy button. The Copy Node page appears as Figure 10-7 shows.

Figure 10-7: Copy Node Page



Copy Node

Specify the name of the new node

From : SunOS 5.8

To :

Hide Options

Copy Subnode

○ yes

● no

4. Enter a name for this node. Remember that this node name must be unique. The limit is 225 characters.
5. Select Yes to copy any subnodes. Select No if you only want to copy this node and no subnodes.

6 Click the Save button. The Applications [*node path*] page appears that displays the information for the newly-copied node, which is now available for editing, deleting, copying, or creating subnodes.

Moving a Node in the Software Tree

The Move Node Wizard allows you to move a node to nearly any other location in the Software Tree. When you move a node to a new destination node, that node becomes a child of the destination node

When you move a node, all of that node’s dependencies and all servers attached to that node remain intact. All other attributes of the node are inherited from the new parent and all direct attachments remain intact.

For example, if you move a node that has servers attached to it, it is likely that the new location will have different packages or custom attributes inherited. That means that the software model has changed and the servers attached to the node need to be reconciled. The Move Node Wizard allows you to perform a reconcile in order to resolve any discrepancies that the move caused.

Restrictions for Moving a Node in the Software Tree

The following list describes the restrictions for moving a node:

- You can only move a node to a location on the Software Tree that has a compatible OS. For example, you cannot move a node that has OS “A” to a node that belongs to OS “B.” However, you can move a node with a specific OS node to a node that is OS independent.
- You can only move a node to a location on the Software Tree that has a compatible customer. For example, you cannot move a node that belongs to Customer A to a node that belongs to Customer B. However, you can move a customer dependent node to a customer independent node.
- You cannot move a node to itself or to a child of itself.
- You cannot move a locked node to a destination node that is not locked, but you can move an unlocked node to a locked node. If you want to move a locked node to another locked node, you need locking permissions to do so.
- You cannot move a top-level node (such as Application Servers, OS Extras, Web Servers, and so on).

- You cannot move nodes within the Hardware and Opsware Software features in the navigational pannel.

How to Move a Node

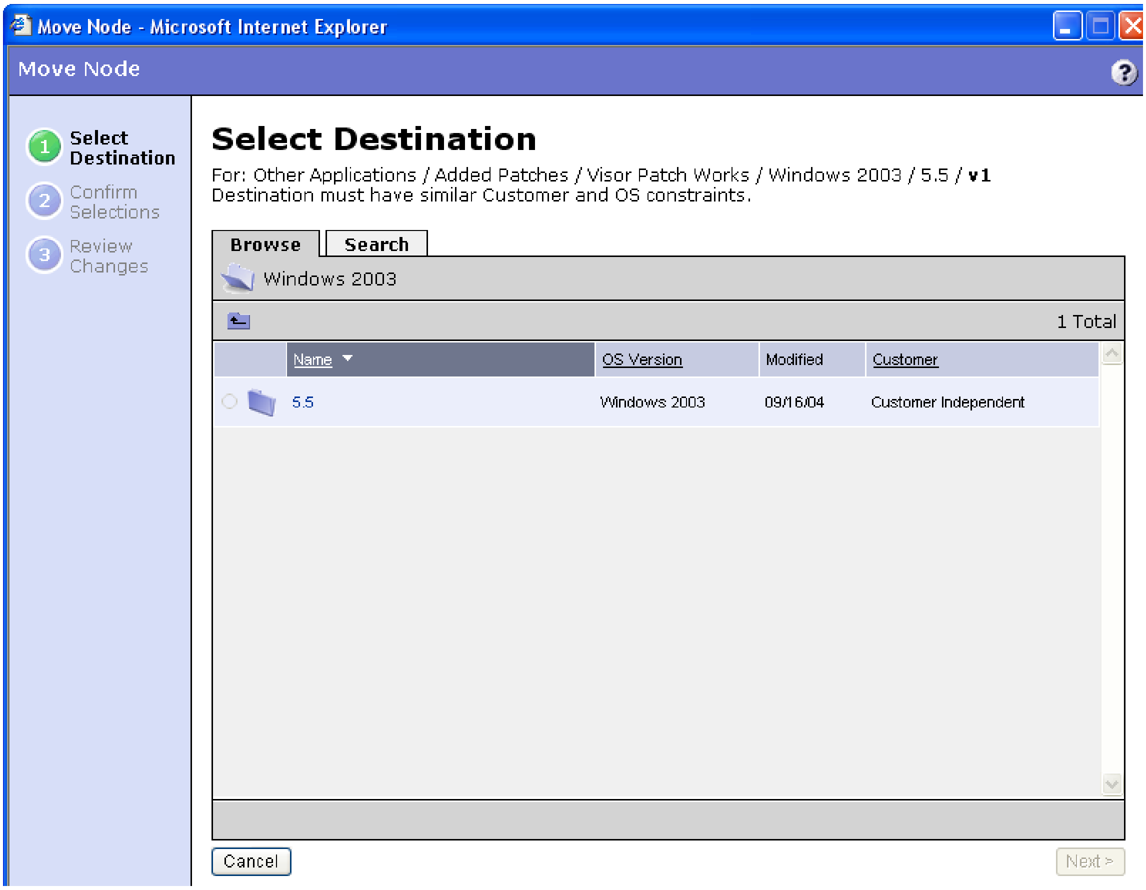
Perform the following steps to move a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.

2. Navigate to the node that you want to move (for example, Application Servers ➤ WebLogic ➤ Solaris 8).

3. Click the Move button. The Move Node Wizard appears.

Figure 10-8: Move Node Wizard, Select Destination page



Select Destination

For: Other Applications / Added Patches / Visor Patch Works / Windows 2003 / 5.5 / **v1**
Destination must have similar Customer and OS constraints.

Windows 2003

1 Total

	Name	OS Version	Modified	Customer
○	5.5	Windows 2003	09/16/04	Customer Independent

4. In the Select Destination page of the wizard, choose a destination for the node. To choose a destination, you have two choices:

- Browse for a Node–From the Browse tab you can browse to a location in the Software Tree by clicking the link of a node's name. When you locate the destination node that you want to move to, select the radio button next to the node name to choose that node as the destination node.
- Search for a Node–If you want to search for a node by name, then select the Search tab. You will notice that the OS and customer criteria are already selected and reflect the properties of the node that you are going to move. To search by name, choose a search criteria (is or contains) from the drop-down list, then enter a name for the node that you would like to search for. In the results page, select a node.

5 Click Next.

6 In the Confirm Selection page of the wizard, check to make sure that you are moving the correct node to the desired destination, and then click Move to move the node.

7 The Review Changes page lists the details of the move node operation. Click Close when you finish.

Managing a Node's Configuration Tracking Policy

The configuration tracking feature allows you to monitor selected configuration files and configuration databases for change and to take certain actions when change is detected.

To use the configuration tracking feature, you create configuration tracking policies, which specify which files to monitor and what actions to take when a change is detected.

The preferred method of creating configuration tracking policies is to use Software Tree nodes. Using nodes allows to you take advantage of the node's model-based architecture. Through nodes, you can create configuration policies and deploy them to the appropriate servers based on what nodes the servers are attached to.

See “Configuration Tracking Setup” on page 387 in Chapter 13 for more information.

Viewing Node History

Using the Opsware Command Center, you can view the audit trail for changes made to a node. For example, you can see who has modified the node that you are browsing.

Most actions performed on the node through the Opsware Command Center are recorded in the history. The following list describes the actions that create an entry in the history for a node:

- Editing any of the node's attributes such as name, description, notes, locked, allow servers, customers, or operating systems
- Adding software to or removing software from the node
- Moving the node
- Changing the software inheritance for the node
- Creating or deleting subordinate nodes
- Moving servers from one node to another
- Adding servers to or removing servers from the node

Each history entry contains three pieces of information, as Table 10-3 shows.

Table 10-3: History Entry Information

HISTORY ENTRY	DESCRIPTION
Event Description	Description of operation performed, for example: Updated lc_certified field to "true"
Modified By	User name of individual who made the change
Date Modified	Date change was made, for example: 18-Aug-2003 08:54:37 PM

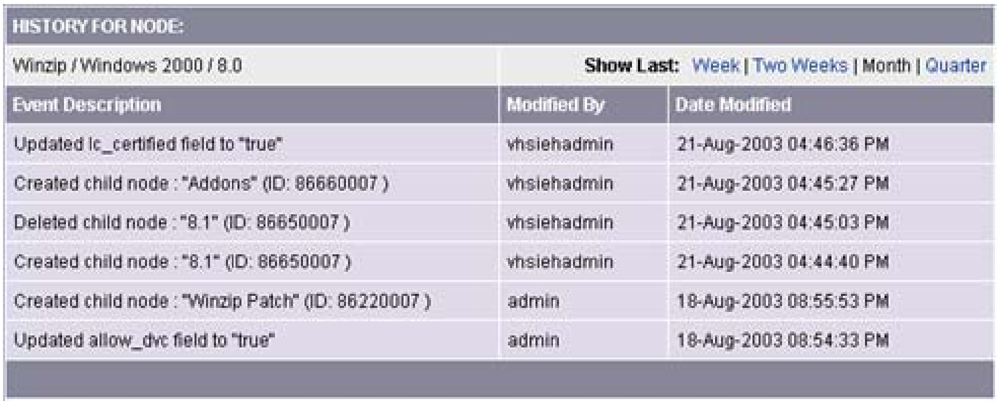
The history is read-only.

Perform the following steps to view the History for Node page:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the level in the node hierarchy where you want to view the history (for example, Application Servers ➤ WebLogic ➤ Solaris 8).

3 Click the History tab. The History for Node page appears, as Figure 10-9 shows.

Figure 10-9: History for Node Page



HISTORY FOR NODE:

Winzip / Windows 2000 / 8.0

Show Last: Week | Two Weeks | Month | Quarter

Event Description	Modified By	Date Modified
Updated lc_certified field to "true"	vhsiehadmin	21-Aug-2003 04:46:36 PM
Created child node : "Addons" (ID: 86660007)	vhsiehadmin	21-Aug-2003 04:45:27 PM
Deleted child node : "8.1" (ID: 86650007)	vhsiehadmin	21-Aug-2003 04:45:03 PM
Created child node : "8.1" (ID: 86650007)	vhsiehadmin	21-Aug-2003 04:44:40 PM
Created child node : "Winzip Patch" (ID: 86220007)	admin	18-Aug-2003 08:55:53 PM
Updated allow_dvc field to "true"	admin	18-Aug-2003 08:54:33 PM

By default, the view shows changes made within the past week. To see changes earlier than the past week, select Two Weeks, Month, or Quarter.

The Opsware Command Center only maintains the history of changes for the last three months.

Software Attached to Nodes

This section provides information about software that is attached to nodes within Opsware SAS and contains the following topics:

- Overview of Software Attached to Nodes
- Modeling Software in Nodes
- Software Configuration Settings
- Viewing Software Attached to a Node
- Adding Package to a Node
- Removing a Package from a Node
- Changing the Installation Order of Software
- How Software Is Inherited from Other Nodes
- Changing the Override Values of Inherited Software

- Dependencies Between Nodes for Software Installation
- Viewing Software Installation Dependencies
- Adding Software Installation Dependencies
- Removing Software Installation Dependencies

Overview of Software Attached to Nodes

Packages are attached to nodes. Using nodes to install packages provides an automated and consistent mechanism for software installation based on the best practices that your organization defines.

See “Overview of Package Management” on page 187 in Chapter 7 for information about how to manage (upload and download) packages through the Opsware Command Center.

A user installs software on a server by using packages stored in the Software Repository. In the Opsware Command Center, the user adds a package to a node and then attaches a server to that node. When the user uses the Install Software Wizard, Opsware SAS reconciles the server and installs the software on the server. See the *Opsware® SAS 5.2 User’s Guide*for more information about Reconcile.

After you define the software directly attached to a node, the packages might not be listed in the order in which they need to be installed on a server. This condition can be true if you recently added new packages to the list. Using the Up and Down arrows next to the package list, you can change the installation order of the packages.

When you modify software that belongs to a node, remember to click the Save Edits button or the changes are not saved.

You can save software edits made to a particular node and commit them all at once. For example, you can add packages, remove packages, move packages up and down in the installation order, reverse the override value on inherited software, and then click the Save Edits button to commit all the changes at the same time. See “How Software Is Inherited from Other Nodes” on page 282 in this chapter for more information.

Modeling Software in Nodes

Opsware SAS supports Advanced IBM Unix (AIX), Hewlett-Packard Unix (HP-UX), Linux, Solaris, and Windows operating systems. Each software package and each node has operating system attributes associated with it. The types of packages users attach to nodes vary by operating system. See “Software Provisioning Setup” on page 247 in this chapter for more information about the full list of package types that Opsware SAS manages.

Table 10-4 shows only the package types that you can attach to nodes.

Table 10-4: Package Types Organized by Operating System

PACKAGE TYPE	FILE FORMATS	NOTES
AIX		
AIX Update Fileset	N/A	None
AIX Base Fileset	N/A	None
AIX APAR	N/A	Users can attach complete and incomplete APARs to nodes. An APAR is incomplete when Opsware SAS does not have all required update filesets for the APAR. Users can install incomplete APARs on servers when the Software Repository contains the update filesets corresponding to the installed base filesets. Possibly, the missing update filesets are not applicable because their base filesets have not been installed. Opsware SAS warns users when they try to reconcile servers when necessary update filesets have not been uploaded.
RPM	.rpm	None
HP-UX		
HP-UX Product	N/A	When products are installed, all filesets that make up that product are installed automatically.
HP-UX Fileset	N/A	None
HP-UX Patch Product	N/A	None

Table 10-4: Package Types Organized by Operating System

PACKAGE TYPE	FILE FORMATS	NOTES
Linux		
RPM	.rpm	None
Solaris		
Solaris Patch	.tar,.tar.Z, .zip, .tar.gz, .tgz, .jar	None
Solaris Patch Cluster	.tar, .tar.Z, .zip, .tar.gz, .tgz, .jar	None
Solaris Package	Datastream File	Opsware SAS supports interactive (requires a response file) and non-interactive Solaris packages.
Solaris Package Instance	N/A	If a Solaris package requires a response file, add it to the package after you upload the package. Attaching an interactive package to a node includes the response file. You do not need to attach the response file to the node. See “Editing Package Properties” on page 217 in Chapter 7 for information about adding a response file for a Solaris package.
RPM	.rpm	None
Windows		
Windows Hotfix	.exe	None
Windows MSI	.msi	None
Windows OS Service Pack	.exe	None
Windows ZIP File	.zip	None

Software Configuration Settings

Each package should contain the configuration settings necessary to run the application on a server. If a configuration change is required in an operational environment, Opsware Inc. recommends that you repackage the software and add the updated package to the Software Repository.

See “Package Management” on page 187 in Chapter 7 for information about how to manage (upload and download) packages with the Opsware Command Center.

System administrators or operations personnel might need to adjust the configuration settings on a server after it is provisioned with an application. Operations personnel might have to further modify configurations after a server is deployed to the environment. As a result, Opsware SAS might be unable to rebuild a server to its latest configuration. Be sure to backup any manual configuration changes.

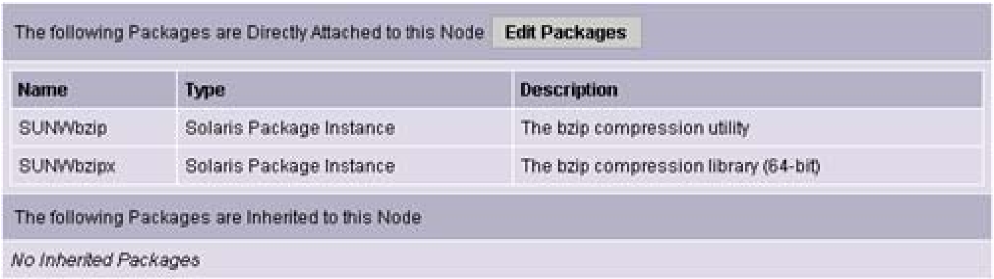
Even though the Opsware Command Center allows users to edit nodes, use caution when you modify existing nodes that have servers attached, so that you preserve the ability to rebuild server configurations.

Viewing Software Attached to a Node

Perform the following steps to view software that is attached to a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to a node (for example, Application Servers ➤ WebLogic ➤ Solaris 8).
3. Click the Packages tab. The Packages Attached to a Specific Node page appears, as Figure 10-10 shows.

Figure 10-10: Packages Attached to a Specific Node



The following Packages are Directly Attached to this Node

Name	Type	Description
SUNWbzip	Solaris Package Instance	The bzip compression utility
SUNWbzipx	Solaris Package Instance	The bzip compression library (64-bit)

The following Packages are Inherited to this Node

No Inherited Packages

This page has the following two sections:

- Package Directly Attached – Directly attached packages are software that is attached specifically at this particular point in the node hierarchy.
- Package Inherited – Inherited Packages are software that is attached at some point higher in the node hierarchy. Inherited software can come from a parent node or from any ancestral node and also can be a combination of packages from several levels of nodes.

Adding Package to a Node

Each package and each node has customer and operating system attributes associated with it. These attributes must match in order for the software to attach to a node. For example, software with a Solaris operating system (Sun Solaris node) cannot be attached to a node associated with a Linux operating system. You cannot attach software to a node that is associated with the operating system OS Independent.

Opsware SAS provides two methods to add a software package to a node. You can use any one method to add a software package to a node and both the methods yield the same results.

Method 1: Adding a Package to a Node

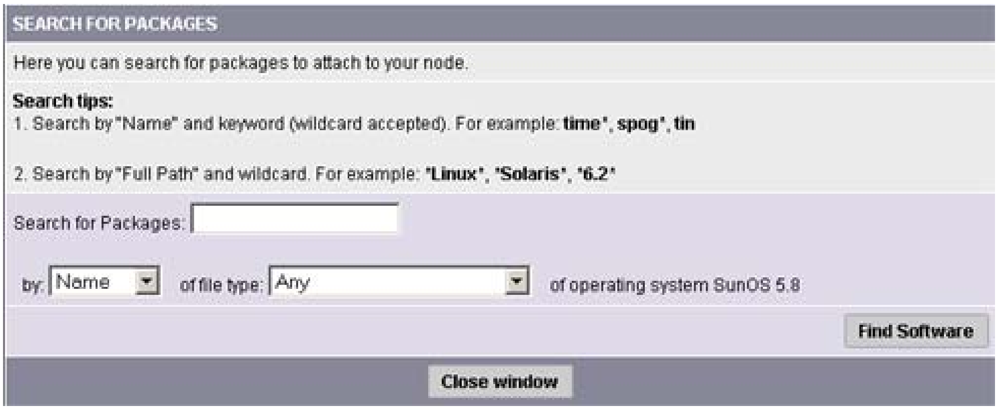
Perform the following steps to add a package to a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to a node (for example, Application Servers ➤ WebLogic ➤ Solaris 8).
3. Click the Packages tab. A page that lists the software attached to the node appears.
4. Click the Edit Packages button. A page appears that shows the directly attached packages and the inherited packages.

When a node contains a large number of packages, the page might take a few seconds to load.

5 Click the Add Packages button. The Search for Packages page appears that allows you to search for the software that you want to add, as Figure 10-11 shows.

Figure 10-11: Search for Packages Form



SEARCH FOR PACKAGES

Here you can search for packages to attach to your node.

Search tips:
1. Search by "Name" and keyword (wildcard accepted). For example: **time*, spog*, tin**

2. Search by "Full Path" and wildcard. For example: ***Linux*, *Solaris*, *6.2***

Search for Packages:

by: Name of file type: Any of operating system SunOS 5.8

6 Search by the package name (if you know it), or search by the path (if you know the directory of the package in the Software Repository).

7 After you specify your search criteria, click the Find Software button.

The time it takes the Opsware Command Center to return search results depends on the number of items a search query needs to process. The more general the query, the slower the results will be. If the query results in more than 500 packages found, the following message appears, “Your search returned too many results. Please try to narrow your query.”

8 From the search results list, select the packages that you want to add to a node by selecting the check box next to each package. (Packages already attached to the node do not have a check box.)

9 Click the Add to Node button. A dialog box appears, which prompts you to search for additional packages.

10 Click Cancel to end your search or click OK to continue searching for additional packages to add to the node.

The packages are added to the end of the list of packages already attached. If you need to specify a different installation order for the packages, use the Move functions. See “Changing the Installation Order of Software” on page 281 in this chapter for more information.

11 Click the Save Edits button.

Additions and changes are not stored in Opsware SAS until you click the Save Edits button.

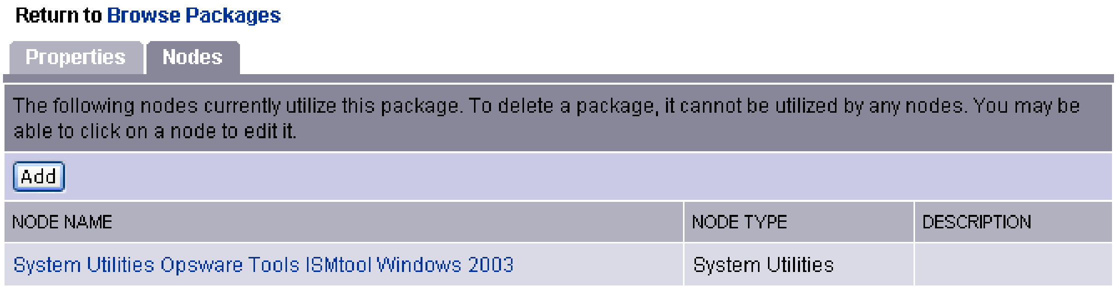
Method 2: Adding a Package to a Node

1 From the navigation panel, click Software ➤ Packages. The Packages: Browse Packges page appears.

2 Select the package. The Packages: Edit Properties page appears.

3 Click the Nodes tab. The Package: View Nodes page appears, as Figure 10-12 shows.

Figure 10-12: The Package:View Nodes Page



The following nodes currently utilize this package. To delete a package, it cannot be utilized by any nodes. You may be able to click on a node to edit it.

NODE NAME	NODE TYPE	DESCRIPTION
System Utilities Opsware Tools ISMtool Windows 2003	System Utilities	

4 Click the Add button. The Add Node to Package window appears.

5 Navigate to a node (for example, Application Servers ➤ WebLogic ➤ Solaris 8). After you have selected the application, click the Select button. The Add Node to Package window displays the package added to the node.

6 Click Close to finish.

Details: Searching for Software Packages

You can search by package name or full path, use wildcards in your search terms, and narrow search results by specifying the file type (RPM, Windows Hotfix, and so forth) of a package. Only file types that are valid for the current node's operating system are available as choices.

- If you know the exact path of the package that you want to attach, you can enter that path in the search box. Change the first drop-down menu to Full Path, and then click the Find Software button. For example:

  ```
  /osimage/Linux/6.2/LC-1.0/cdrom/RedHat/RPMS/vixie-cron-
  3.0.1-40.i386.rpm
  ```

- If you know the name of the package, but not its location, set the first drop-down menu selection to Name and search for just the name of the software (without version information or file extension). For example:

  ```
  vixie-cron
  ```

- If you want to find all packages that start with a certain string, set the first drop-down menu selection to Name, type a wildcard query string, and click Find Software. For example:

  ```
  time
  ```

  (You do not need to type the wildcard character "*" in this case.)

- If you want to find all the packages that are located in a particular directory, set the first drop-down menu selection to Full Path and search for a wildcard query string that specifies the directory that you want. For example:

  ```
  *RedHat*
  ```

Removing a Package from a Node

Users can delete one, many, or all of the packages attached to a node. Be careful because deleting software from nodes might cause problems for other users of the same nodes. Check with other users who might be using the nodes before you delete any associated software.

Perform the following steps to remove a package from a node:

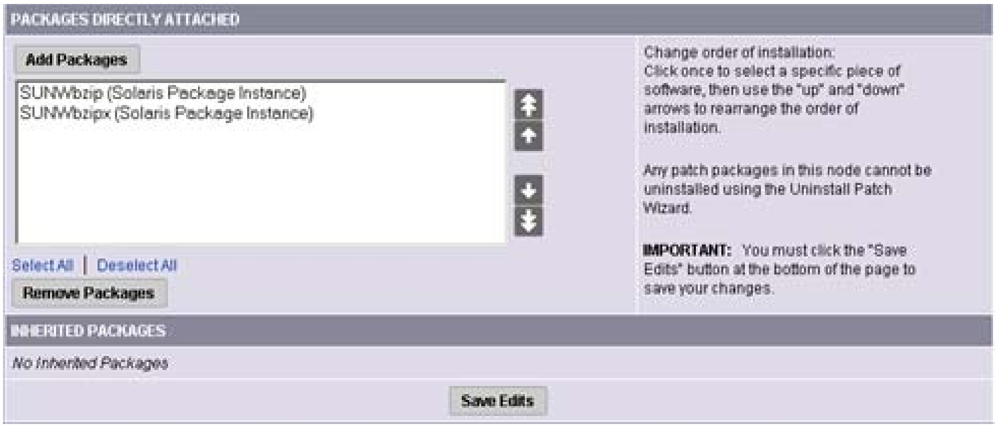
1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.

2. Navigate to a node (for example, Application Servers ➤ WebLogic ➤ Solaris 8).

3 Click the Packages tab. A page appears that shows the list of packages attached to the node.

4 Click the Edit Packages button. A page appears that shows a form with the packages currently attached displayed inside a box that allows additional packages to be added, the order of the packages to be changed, or packages to be removed, as Figure 10-13 shows.

Figure 10-13: Edit Packages Page


PACKAGES DIRECTLY ATTACHED
Add Packages
SUNWbzip (Solaris Package Instance)
SUNWbzipx (Solaris Package Instance)
Select All | Deselect All
Remove Packages
INHERITED PACKAGES
No Inherited Packages
Save Edits

Change order of installation:
Click once to select a specific piece of software, then use the "up" and "down" arrows to rearrange the order of installation.

Any patch packages in this node cannot be uninstalled using the Uninstall Patch Wizard.

IMPORTANT: You must click the "Save Edits" button at the bottom of the page to save your changes.

5 Click the package name in the Packages Directly Attached box to highlight the package to be deleted.

You can highlight all the packages at one time by clicking the Select All button located below the list. (You can also reset the selection by clicking the Deselect All button.) You can select multiple packages to delete by holding down the CTRL key while selecting packages.

6 Click the Remove Packages button.

The selected packages disappear from the select box but the packages are not yet detached from the node.

7 Click the Save Edits button at the bottom of the page to complete detachment of the software.

Additions and changes are not stored in Opsware SAS until you click the Save Edits button.

To apply changes that you made to a node to servers that already have the node attached, you need to reconcile those servers. See the *Opsware® SAS 5.2 User's Guide* for more information about Reconcile.

Changing the Installation Order of Software

Perform the following steps to change the installation order of the software:

1 From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.

2 Navigate to a node (for example, Application Servers ➤ WebLogic ➤ Solaris 8).

3 Click the Packages tab. A page appears that shows the list of packages attached to the node.

4 Click the Edit Packages button. A page appears that shows a form with the packages currently attached displayed inside a box that allows additional packages to be added, the order of the packages to be changed, or packages to be removed.

5 Highlight the single package or multiple packages (Ctrl-Click) that you want to move in the installation order.

6. Click the up arrow button or the down arrow button.

   Highlighted packages are moved up or down one position in the installation order each time you click the button.

   Click the move to top arrow button or move to bottom arrow button.

   Highlighted packages are moved to the top or bottom of the installation order.

7. When you finish making changes to the installation order, click the Save Edits button at the bottom of the page.

Installation order changes are not stored in Opsware SAS until you click the Save Edits button.

How Software Is Inherited from Other Nodes

If a node inherits software from its parent (or from a node farther up the node hierarchy), the software displayed for the node includes directly attached software as well as software inherited from parent nodes. For the inherited software, you can override whether or not software is installed by the current node, but you cannot change the order of the inherited packages.

When you reconcile, inherited software is installed first, then directly attached software is installed.

Examples: Ways to Use Inheritance for Software

A subordinate node can inherit the properties of a parent node. For example, IIS only runs on Windows NT. The parent node indicates that the operating system for the node is Windows NT only. The subordinate nodes created under that node can only be used for Windows NT servers.

In a second example, you create a node for a version of IIS (version 1). Then, you create a subordinate node and attach IIS version 1.1, which has the same list of software except that it adds a few more packages. The subordinate node of IIS inherits the list of software that is attached to the node for version 1.

A third way that you can use inheritance is for installing and testing new versions of software. For example, you might create a subordinate node (Q1) of the node (Q) that contains software to be updated or patched. You could then move a group of test servers from node Q to the subordinate node Q1. In the inherited software list of Q1, you could override packages that contain changed software, so as not to inherit similar packages from the parent node. Then, you can directly attach the new packaged version of the software to Q1. When you reconcile, the overridden package is removed from the test servers and the new directly attached package is installed instead.

Changing the Override Values of Inherited Software

In the inherited software list, most of the packages have a plus symbol (+) to the left. These packages are referred to as *plus override*. Any software package with a plus symbol (+) by its name is inherited and installed on servers attached to this node.

If a software package has a minus symbol (–) to the left of its name, it is referred to as *minus override*. This means that the node is aware that its parent has a particular package, but the node does not inherit this package and servers attached to the node do not have this package installed.

Perform the following steps to change the override values of inherited software:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.

2. Navigate to a node (for example, Application Servers ➤ WebLogic ➤Solaris 8).

3. Click the Packages tab. A page appears that shows the list of packages attached to the node.

4. Click the Edit Packages button. A page appears that shows a form with the packages currently attached displayed inside a box that allows additional packages to be added, the order of the packages to be changed, or packages to be removed.

5. In the Inherited Packages box, highlight one package at a time or select multiple packages (Ctrl-Click) for which you want to change override settings.

6. When you finish your selection, click the Save Edits button.

   Selected packages that were prefaced with a plus symbol (+) are prefaced with a minus symbol (–), and packages that were prefaced with a minus symbol (–) are prefaced with a plus symbol (+).

7. Click the Save Edits button.

The changes made to override values are not committed to Opsware SAS until you click the Save Edits button.

After the edits are saved, the page refreshes, updated to show your changes.

Dependencies Between Nodes for Software Installation

In addition to specifying installation order for directly attached and inherited software within nodes, users can define special dependencies between nodes to specify the order of software installation on servers. Spelling out any special dependencies that exist for specific packages allows those packages to be installed in the correct order when a server is reconciled.

Opsware SAS reconciles and installs software on servers in the following default order (from first to last):

- Operating System
- OS Extras
- System Utilities
- Database Server
- Application Server
- Web Server
- Other Applications
- Patches

Sometimes the default order needs to be overridden so that packages in one category are installed before another package in a different category. You can prescribe a change from the default package installation order by clicking the Dependency tab and specifying any special dependencies of different nodes. In doing so, you can make one node dependent on another so that the software is installed in the correct order.

For example, if a Web server package and a corresponding application server plug-in package are both installed on the same server, the Web server package must be installed before the application server plug-in (to ensure correct configuration of the plug-in). In that case, you can specify an installation order dependency for plug-ins that Web server packages must be installed before the plug-in packages.

These dependencies are for installation ordering only, not to check for the presence of a particular piece of software.

Viewing Software Installation Dependencies

If the current node is locked (a lock icon displays beside the node name at the top of the page), then only authorized staff can add or remove dependencies. If you have permission to modify node dependencies, you might see two orange buttons at the top of the screen: Remove Dependency and Add Dependency. The Remove Dependency button does not appear if there are no dependencies.

The Opsware Command Center displays a list of nodes that are dependent on the current node. You see a list of nodes that should precede and follow the current node when determining installation order for software attached to those nodes.

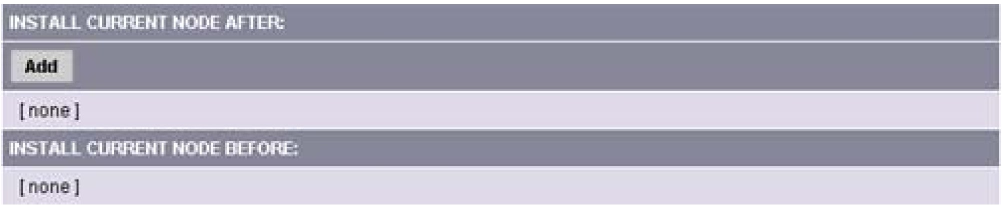
For convenience, each node in each list is a hyperlink. To see details about each node, click the hyperlinked node name.

You cannot remove the Install Order for nodes that are to be installed before the current node. If a dependency listed in this section needs to be removed, you need to go to that node and remove the dependency from that node's Install Order tab.

Perform the following steps to view software installation dependencies:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the node for which you want to view an installation order dependency (for example, Application Servers ➤ WebLogic ➤ Solaris 8).
3. Click the Install Order tab. The Install Current Node After list and Install Current Node Before list display, as Figure 10-14 shows.

Figure 10-14: Install Order Tab



INSTALL CURRENT NODE AFTER:

[none]

INSTALL CURRENT NODE BEFORE:

[none]

The Opsware Command Center displays [none] when there are no installation order dependencies.

Adding Software Installation Dependencies

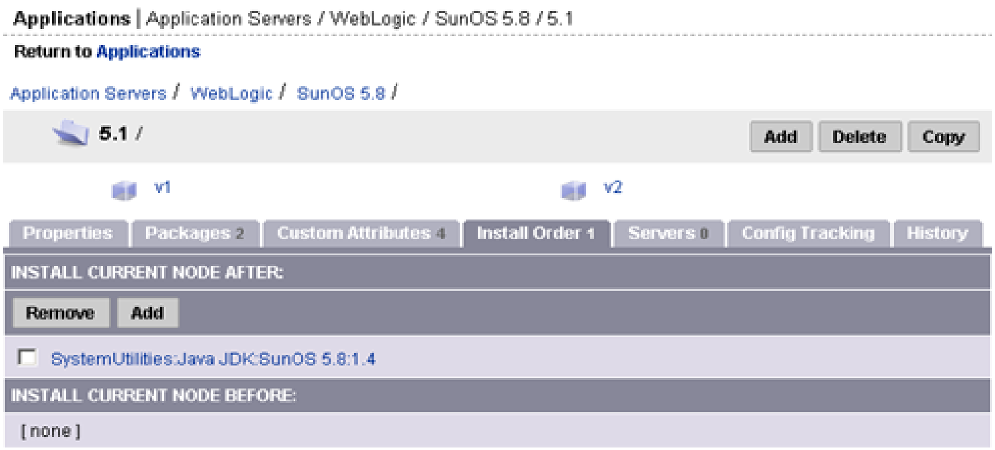
When you create software installation order dependencies, Opsware Inc. recommends that you follow these rules:

- A node cannot be made dependent on itself.
- Do not create a circular dependency between nodes; for example, Node A is dependent on Node B and Node B is dependent on Node A. If a server is attached to a node with a circular dependency and you attempt to reconcile the server, the Opsware Command Center displays an error message and does not complete the reconcile.

Perform the following steps to add software installation dependencies:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the node for which you want to add an order dependency (for example, Application Servers ➤ WebLogic ➤ SunOS 5.8 ➤ 5.1).
3. Click the Install Order tab. The Install After list and Install Before list display.
4. Click the Add button. A window appears that shows the categories.
5. Navigate to the node for which you want to specify an installation order before the current node (for example, System Utilities ➤ Java JDK ➤ SunOS 5.8 ➤ 1.4).
6. Click the Add button. The Opsware Command Center closes the window to display the new software installation order dependency, as Figure 10-15 shows.

Figure 10-15: New Installation Order Dependencies



Applications | Application Servers / WebLogic / SunOS 5.8 / 5.1

Return to Applications

Application Servers / WebLogic / SunOS 5.8 /

5.1 /

INSTALL CURRENT NODE AFTER:

☐ SystemUtilities:Java JDK:SunOS 5.8:1.4

INSTALL CURRENT NODE BEFORE:

[none]

Removing Software Installation Dependencies

You can delete multiple dependencies at the same time by selecting multiple check boxes before you click Remove Dependency.

Perform the following steps to remove software installation dependencies:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the node for which you want to remove an install order dependency (for example, Application Servers ➤ WebLogic ➤ Solaris 8).
3. Click the Install Order tab.
4. Click the check box next to the specific dependency that you want to delete.
5. Click the Remove Dependency button.

Custom Attributes Set for the Environment

This section provides information on custom attributes set for the environment within Opsware SAS and contains the following topics:

- Overview of Custom Attributes Set for the Environment
- Managing Custom Attributes
- Adding Custom Attributes for a Node
- Editing Custom Attributes for a Node
- Deleting Custom Attributes for a Node

Overview of Custom Attributes Set for the Environment

Users might need to store specific miscellaneous information in the Opsware Model Repository, for example, to facilitate server or application installation and configuration or scripting.

The Opsware Command Center provides a data management function that allows users to set custom attributes for servers. These custom attributes include miscellaneous parameters and named data values. Users can write scripts that use these parameters and data values when they perform a variety of functions, including network and server configuration, notifications, and CRON script configuration.

For information about how to set custom attributes required by the software running on a specific server, contact the group responsible for packaging your applications.

Managing Custom Attributes

✓ Even though the Opsware Command Center allows users to edit nodes, use caution when you modify existing nodes, especially those with servers attached, so that you preserve the ability to rebuild server configurations.

To set custom attributes that affect a specific server, attach the custom attributes directly to the specific servers.

See “Setting Custom Attributes for Customers” on page 74 in Chapter 4 for more information about setting custom attributes for customers.

To set custom attributes that affect every server for a customer, you can set custom attributes for that customer.

Adding Custom Attributes for a Node

When you add custom attributes to a node, the attributes and values affect every server attached to that node.

Perform the following steps to add custom attributes for a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.

2. Navigate to the node for which you want to add a custom attribute (for example, Application Servers ➤ WebLogic ➤ Solaris 8).

3. Click the Custom Attributes tab.

   If there are no custom attributes, the button is called Add Custom Attributes. If there are custom attributes and you want to add more, click the Edit Custom Attributes button, and then the Add Custom Attributes button.

4. Enter the name and value for the custom attribute that you want to add. You can enter up to 10 custom attributes.

If you want to enter a value that is longer than the space available in the field, click the "..." button to open a window with a larger text box.

5. Click the Save button. The View Custom Attributes page appears.
6. Click the Edit Custom Attributes button.
7. Click the Save Edits button.

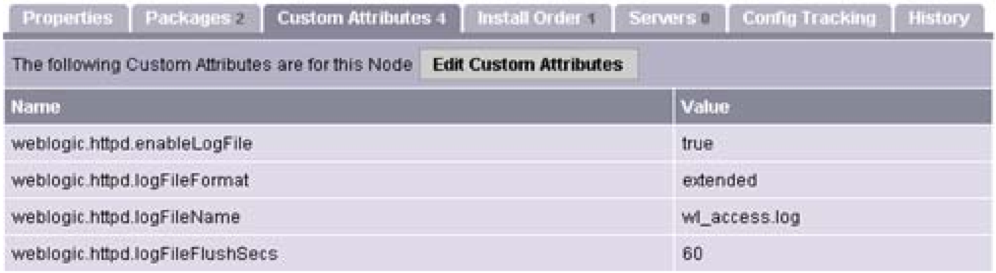
Editing Custom Attributes for a Node

To change the name of a custom attribute entry, create a new custom attribute with the new name and delete the old custom attribute.

Perform the following steps to edit custom attributes for a node:

1. From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.
2. Navigate to the node for which you want to add a custom attribute (for example, Application Servers ➤ WebLogic ➤ Soalris 8).
3. Click the Custom Attributes tab.
4. Click the Edit Custom Attributes button. A new form appears, which shows three columns of information: Name, Inherited Value, and Local Value. See Figure 10-16.

Figure 10-16: Edit Custom Attributes Page



The following Custom Attributes are for this Node

Name	Value
weblogic.httpd.enableLogFile	true
weblogic.httpd.logFileFormat	extended
weblogic.httpd.logFileName	wl_access.log
weblogic.httpd.logFileFlushSecs	60

- Name is the name of the attribute.
- Inherited Value is the value that was entered in an ancestral node for the name that displays.

- Local Value is the value for the current node, which will override the inherited value if one displays.

5 If there are inherited values, the label next to the check box is labeled Inherit. Check it if you want to use the inherited value. If it is not checked, the local value is used.

If there are no inherited values, the label next to the check box is Delete. Check it if you want the attribute to be deleted when the Save Edits button is clicked.

6 If there is an inherited value, and the Inherit check box is checked, the inherited value is the one being used. To override that value, deselect the check box. The Local Value text box is enabled to allow text to be entered.

7 If there is {more...} in the local value text box, the value is too large to put in the text box. To edit this value, select the "..." button to open a window with a larger text entry box.

8 Click the Save Edits button to commit the changes.

The changes made to custom attributes are not committed to Opsware SAS until you click the Save Edits button.

Deleting Custom Attributes for a Node

Perform the following steps to delete custom attributes for a node:

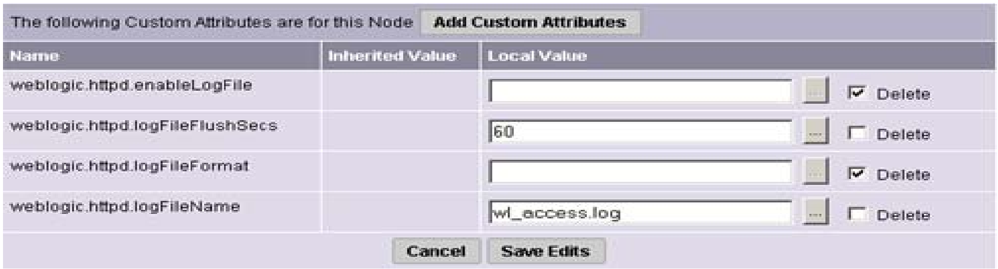
1 From the navigation panel, click Software ➤ Applications. The Applications page appears that shows the categories.

2 Navigate to the node for which you want to delete a custom attribute (for example, Application Servers ➤ WebLogic ➤ Solaris 8).

3 Click the Custom Attributes tab. A page appears that shows the custom attributes for the selected node.

4. Click the Edit Custom Attributes button. The three-column form appears with a check box labeled Delete available next to the Local Value field, as Figure 10-17 shows.

Figure 10-17: Delete Custom Attributes



The following Custom Attributes are for this Node

Name	Inherited Value	Local Value	
weblogic.httpd.enableLogFile			☑ Delete
weblogic.httpd.logFileFlushSecs		60	□ Delete
weblogic.httpd.logFileFormat			☑ Delete
weblogic.httpd.logFileName		wl_access.log	□ Delete

5. Select the check box next to the attributes that you want to delete.

   If the label for the attribute is Inherit, and you check the box, only the local value is deleted. To completely remove an inherited attribute, delete it from the node higher in the hierarchy from which it was inherited.

6. Click Save Edits to commit the change and delete the attributes.

Templates and Folders

This section provides information on how to work with templates within Opsware SAS and contains the following topics:

- Overview of Templates and Folders
- Templates, Folders, and Inheritance
- Template Inheritance
- Attachments: Local, Inherited, and Blocked
- Blocking and Reattaching Inherited Attachments

Overview of Templates and Folders

Opsware templates allow you to create groups of logical relationships between nodes and a server. With templates, you can arrange related sets of packages together so that you can apply them to a server in a single operation by using the Opsware template wizard.

Templates represent collections of objects such as software, service levels, operating systems, and patches that are simultaneously attached to a server when the template is applied. These collections of nodes are referred to as *attachments* in the Templates feature of Opsware SAS. Unlike attaching software to nodes in the software tree, however, templates are applied but do not stay permanently associated with the server.

The two basic types of Opsware templates are:

- Templates that include the installation of an operating system
- Templates that do not include an operating system installation

For example, you can use an Opsware template to quickly bring new servers into production. Such a template might include an operating system for a new server, the latest security patches for the operating system, plus all the applications that are required to run a full-fledged Web service. In another case, you could create a template that consists of a set of applications and patches to install a new service on servers that are already in production.

Templates, Folders, and Inheritance

Using templates and folders, you can create a deep hierarchy of templates to take advantage of commonalities between server configurations. You can add as many subfolders and other templates inside folders as you would like, grouping together any number of templates to be applied simultaneously to a server.

Folders are more than empty containers into which you can organize your templates. They can also have attachments. Importantly, folders operate under the principle of inheritance, which means that any nested folders or templates inherit all the attachments of the parent folder they belong to. Inheritance minimizes the amount of maintenance required to manage templates in a hierarchy.

A unique feature of templates is the ability to apply either a template or a folder to a server. Because a folder can take attachments, the process of selecting and applying the folder is the same as applying a template. It is important to know that templates do not have a persistent connection to the servers they are used to configure. Consequently, changes made to a template do not affect servers that are already configured with that template.

Template Inheritance

Template inheritance works in such a way that templates and folders inherit all attachments of the folder they reside in. Inheritance is propagated from parent (folder) to child (template or folder) – and all children of children. It is important to know that child folders and templates always inherit the attachments of their ancestor folders, unless you specifically block the inheritance of an attachment inside a template or folder.

You can attach the following nodes to a template:

- Operating System (only one per template)
- Applications
- Patches
- Service Levels

You can attach nodes to a folder or template in the following three ways:

- At the current or local level
- At the current level by inheritance from an ancestor folder
- Blocked at the current level

  Blocking at the current level prevents an attachment from being inherited by child folders.

Take care in organizing your folders so that you can take maximum advantage of inheritance when you create child folders. Organize your folders so that the most common attachments that servers use are contained in the parent folders. That means no matter how many child folders are created from that parent, if an attachment needs to change in all folders in a family, you only need to make that change once, in the parent folder, and all child folders and child templates will inherit the change.

Attachments: Local, Inherited, and Blocked

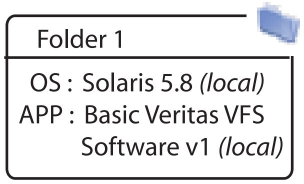
Templates take advantage of commonalities among server configurations. You can use the power of inheritance to further minimize maintenance of your templates as configurations need to change. This section discusses how to define attachments to achieve this goal.

All attachments in a folder are automatically propagated to any child folders or templates. The three possible states that an attachment can be in are *local*, *inherited*, or *blocked*.

Local

If a node is attached directly to a folder or a template, the attachment is considered *local*, which means that the attachment is not inherited from an ancestor folder. It is directly attached to the folder. Figure 10-18 shows that Solaris 5.8 and Basic Veritas VFS Software v1 are attached locally to Folder 1.

Figure 10-18: Folder with Nodes Attached Locally



This form of attachment is the simplest. Understanding local attachments is important, as more complex examples are shown.

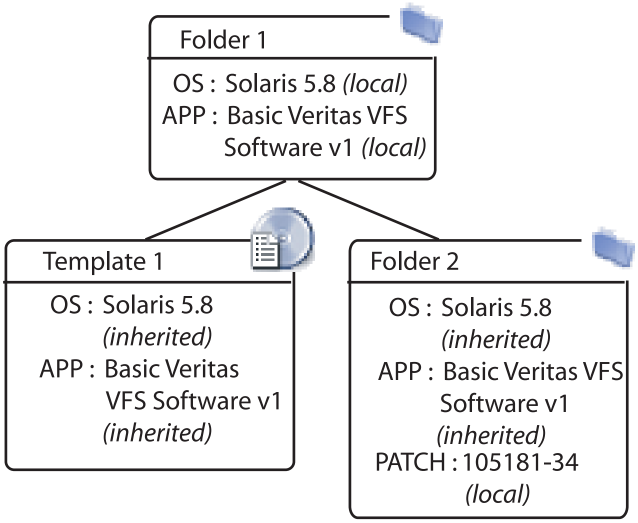
Inherited

If an attachment is not attached locally to a folder or a template, but is inherited from an ancestor folder, the attachment is considered *inherited*.

Figure 10-19 shows that Folder 1 from the previous diagram now has a child Folder 2 and a child Template 1. The major difference between the two children–the folder and the template–is that you can further customize the folder with more levels of folders and templates, while you cannot do that to the template.

Both the template and the folder inherit Solaris 5.8 and Basic Veritas VFS Software v1 from the parent folder, plus Template 1 has the Patch 105181-34 attached locally that is inherited by its children, as Figure 10-19 shows.

Figure 10-19: Folder with a Child Folder and a Template Showing Attachments Inherited from the Parent Folder


Folder 1
OS : Solaris 5.8 (local)
APP : Basic Veritas VFS Software v1 (local)
Template 1
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v1 (inherited)
Folder 2
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v1 (inherited)
PATCH : 105181-34 (local)

Applying Folder 2 to a group of servers configures them with the inherited OS (Solaris 5.8) and the Basic Veritas VFS Software v1, in addition to the one patch. At this point, you could use either Folder 1 or Template 1 with the same results.

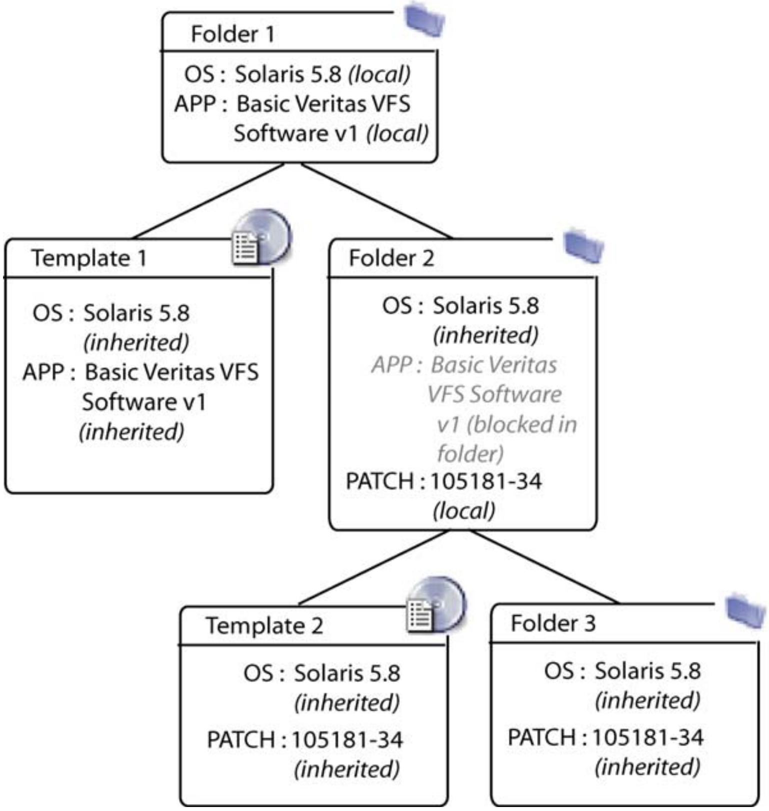
Blocked

You can also block an attachment, which means that it is not installed when that template is applied. Also, blocked attachments do not appear in child templates or folders.

Figure 10-20 shows Template 1 and Folders 1 and 2 from the previous example, but now Basic Veritas VFS Software v1 has been blocked. Consequently, the children created under it, Template 2 and Folder 3, do not inherit that application.

You can only block inherited attachments. You can delete local attachments and their inheritance down the tree is removed. If the parent has an attachment, and you do not want the children to have it, use blocking to prevent it from propagating to its children.

Figure 10-20: Folders with Child Folders and Templates That Show Attachments Blocked from Inheritance


Folder 1
OS : Solaris 5.8 (local)
APP : Basic Veritas VFS Software v1 (local)
Template 1
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v1 (inherited)
Folder 2
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v1 (blocked in folder)
PATCH : 105181-34 (local)
Template 2
OS : Solaris 5.8 (inherited)
PATCH : 105181-34 (inherited)
Folder 3
OS : Solaris 5.8 (inherited)
PATCH : 105181-34 (inherited)

Blocking and Reattaching Inherited Attachments

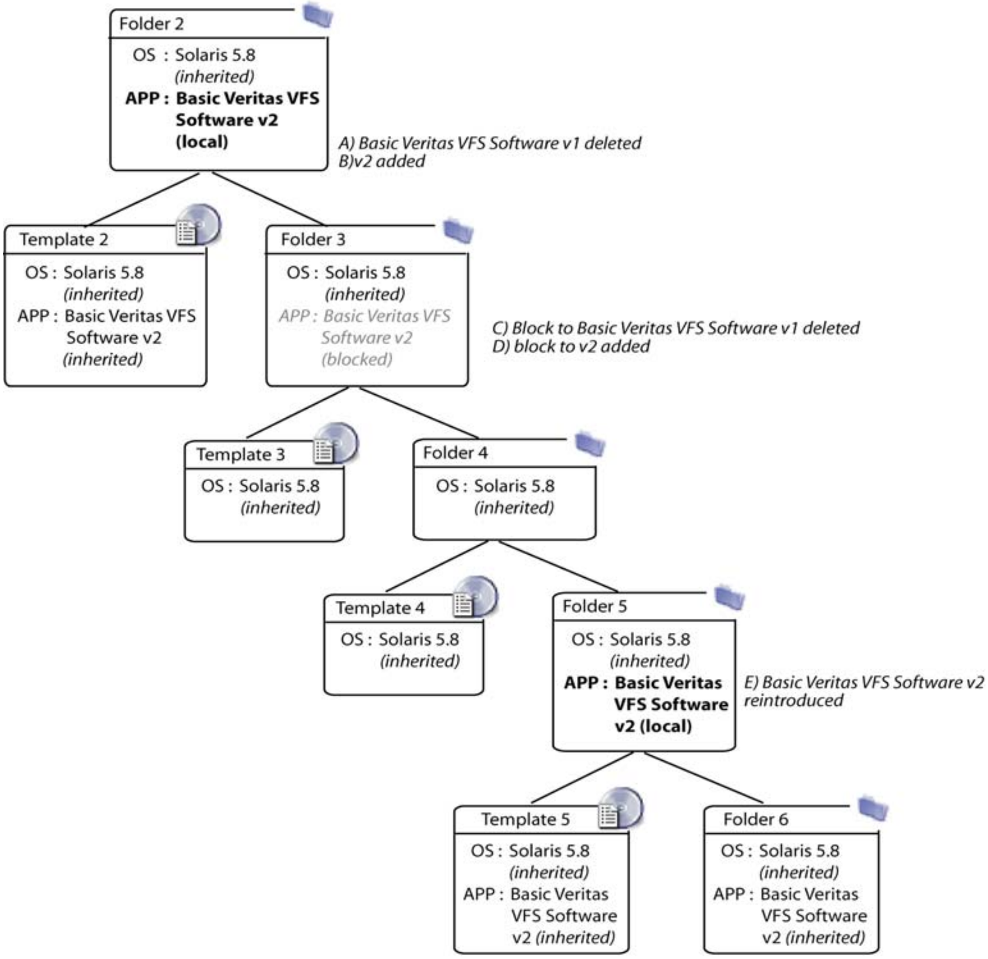
Blocking and then reattaching an attachment lower in the tree is possible, but this action can be complex and should be done with care.

An attachment that you block in an ancestor folder is not inherited by the children of that folder. You can add the blocked attachment again to a folder or template lower down the hierarchy, and that attachment is again inherited by children still farther down the hierarchy, until it is blocked.

In Figure 10-21, you can see in Step A a new version of Basic Veritas VFS software that is attached to Folder 2, called v2. Template 2 inherits this new version. But the block on Folder 3 would not apply the v2 software to Folder 3, and subsequently, all children of Folder 3 do not inherit this new version of the Veritas software.

In order for other children in the hierarchy to inherit the Veritas v2 software, you would need to reintroduce (reattach) the software into a child folder. The diagram in Figure 10-21 shows how Folder 5 has had the Veritas software reintroduced, and thus all children of Folder 5, Template 5 and Folder 6, now inherit the new version of the Veritas software.

Figure 10-21: Example of Blocked-Unblocked Attachments in a Template Folder Hierarchy


Folder 2
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v2 (local)
A) Basic Veritas VFS Software v1 deleted
B)v2 added
Template 2
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v2 (inherited)
Folder 3
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v2 (blocked)
C) Block to Basic Veritas VFS Software v1 deleted
D) block to v2 added
Template 3
OS : Solaris 5.8 (inherited)
Folder 4
OS : Solaris 5.8 (inherited)
Template 4
OS : Solaris 5.8 (inherited)
Folder 5
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v2 (local)
E) Basic Veritas VFS Software v2 reintroduced
Template 5
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v2 (inherited)
Folder 6
OS : Solaris 5.8 (inherited)
APP : Basic Veritas VFS Software v2 (inherited)

Delete old attachments before you attach the new version.

Blocks do not disappear automatically when you delete the related local attachment. An *orphan* block (one with no local attachments of the same kind) does not affect the system.

Working with Folders and Templates

This section provides information about folders and templates within Opsware SAS and contains the following topics:

- Overview of Folders and Templates
- Applying Templates and Folders
- Creating Templates
- Creating Folders
- Operating System in Templates or Folders
- Copying Templates and Folders
- Deleting Templates or Folders
- Blocking Folders and Templates from Inheriting
- Blocking vs. Removing Attachments

Overview of Folders and Templates

Opsware SAS allows you to create both folders and templates. Create folders when you plan to develop a hierarchy that uses inheritance to define generalized parent folders with increasingly specific child folders below. Create templates when you need only a single level of attachments to be defined and you do not need those attachments to be inherited. If later you decide that you want a template to become a folder so that you can build a hierarchy and use inheritance, you can copy the template as a folder and make that copy a folder.

Consider creating folders instead of templates to allow for the future growth of your folder hierarchy.

You can specify an operating system version and customer for the folder or template, and Opsware SAS only allows the combination of operating system and customer for the child templates and folders.

Folders and templates require little setup and you can create and deploy them quickly. When you create a folder or template, you select applications, patches, operating systems, or service levels that are already configured and tested for installation, and add them to the folder or template. If, for example, a new patch is released, you can edit the folder or template and add the new patch. Any application of the template to a server would then include the patch.

Applying Templates and Folders

If the template that you create includes an operating system, the template is applied through the Install OS Wizard. If the template you create does not include an operating system (OS Independent), the template is applied through the Install Template Wizard.

If you edit a template, the changes only affect new applications of the template. Servers that already had the template applied are not automatically modified to match the changed template.

Creating Templates

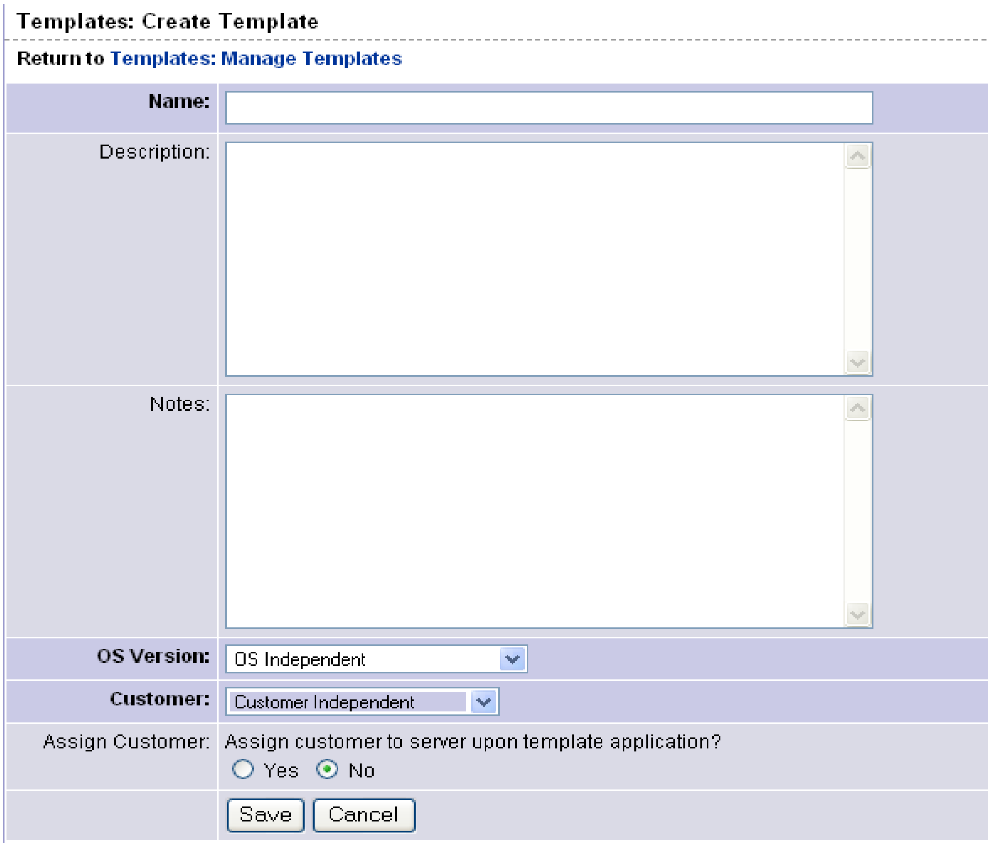
Perform the following steps to create a template:

1 In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

  You can either create a new template here or navigate to the location in the folder hierarchy where you would like to create the new template.

2. Click the New Template button. The Templates: Create Template page appears, as Figure 10-22 shows.

Figure 10-22: Templates: Create Template Page



Templates: Create Template

Return to Templates: Manage Templates

Name:

Description:

Notes:

OS Version: OS Independent

Customer: Customer Independent

Assign Customer: Assign customer to server upon template application?

○ Yes ● No

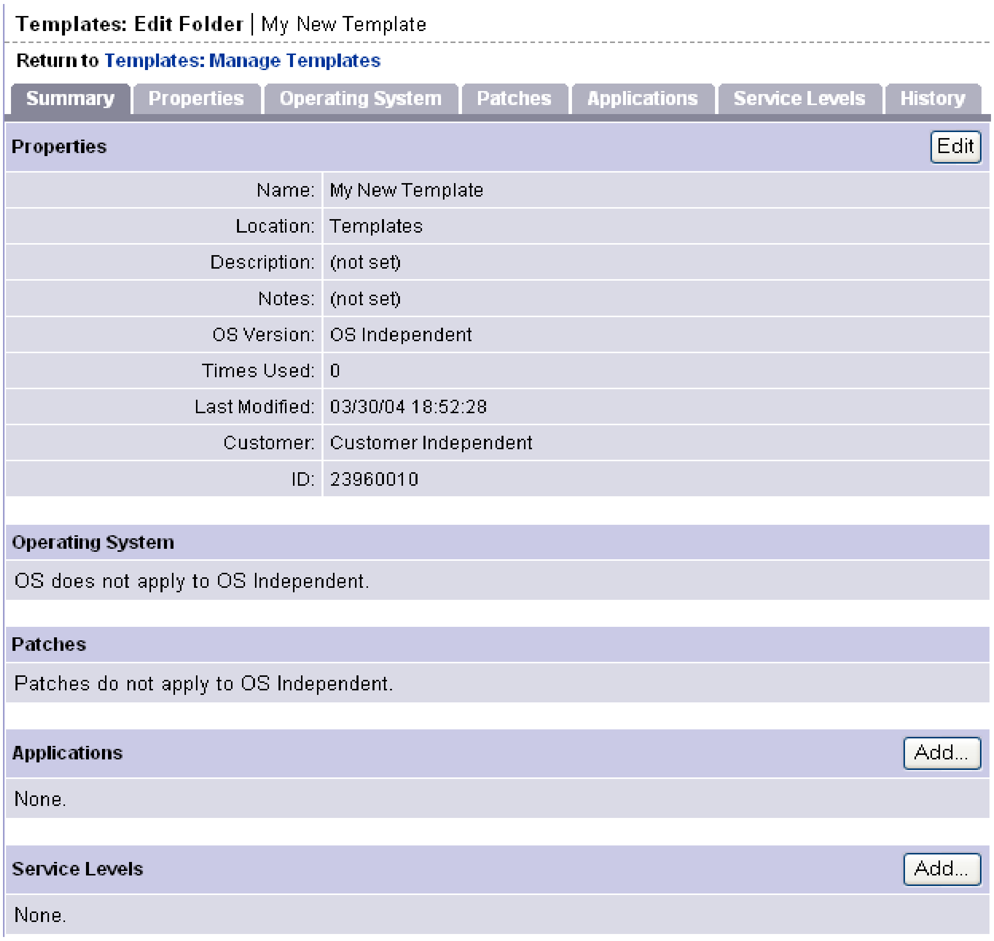
3. Enter a name for the template and then select an operating system version and a customer (all required.) You can also provide a description of the template.

4. If you want the server to which you apply the template to be automatically assigned to the customer associated with the template, select the Yes option in the Assign Customer field.

If the server is already assigned to a customer, selecting this option causes the server to be reassigned when the template is installed.

5 Click Save to create the template. The Templates: Edit Folder | <Template Name> page appears, as Figure 10-23 shows.

Figure 10-23: Templates: Edit Folder | Template Name Page



Templates: Edit Folder | My New Template

Return to Templates: Manage Templates

Properties

Name:	My New Template
Location:	Templates
Description:	(not set)
Notes:	(not set)
OS Version:	OS Independent
Times Used:	0
Last Modified:	03/30/04 18:52:28
Customer:	Customer Independent
ID:	23960010

Operating System

OS does not apply to OS Independent.

Patches

Patches do not apply to OS Independent.

Applications

None.

Service Levels

None.

You can now select the operating system, patches, applications, and service levels that you want to add to the template.

Creating Folders

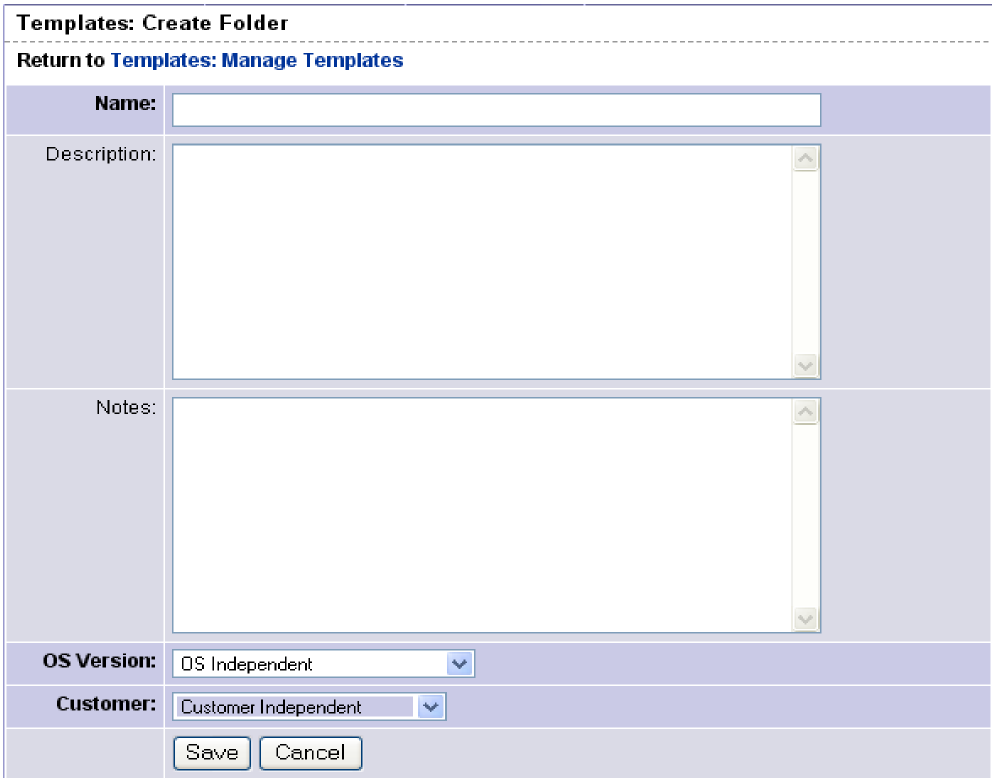
Perform the following steps to create a folder:

1 In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

You can either create a new folder here or navigate to the location in the hierarchy where you would like to create the new folder.

2 Click the New Folder button. The Templates: Create Folder page appears, as Figure 10-24 shows.

Figure 10-24: Templates: Create Folder Page



Templates: Create Folder

Return to Templates: Manage Templates

Name:

Description:

Notes:

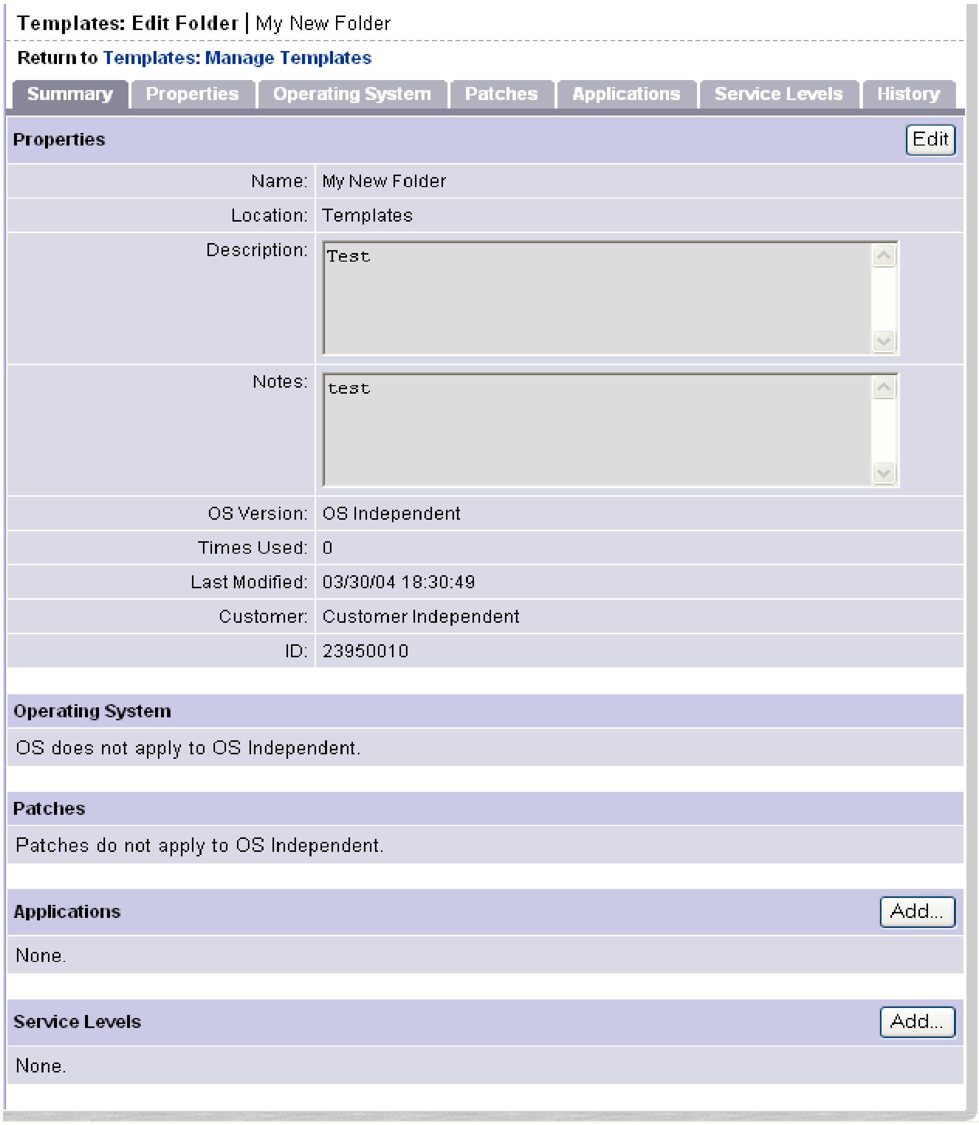
OS Version: OS Independent

Customer: Customer Independent

3 Enter a name for the folder, select an operating system version and select a customer (all required). Optionally, you can add a description and notes.

4 Click Save. The new folder is created and the Templates: Edit Folder | <Folder Name> page appears, as Figure 10-25 shows.

Figure 10-25: Templates: Edit Folder | Folder Name Page



Templates: Edit Folder | My New Folder

Return to Templates: Manage Templates

Properties

Name: My New Folder

Location: Templates

Description: Test

Notes: test

OS Version: OS Independent

Times Used: 0

Last Modified: 03/30/04 18:30:49

Customer: Customer Independent

ID: 23950010

Operating System

OS does not apply to OS Independent.

Patches

Patches do not apply to OS Independent.

Applications

None.

Service Levels

None.

Operating System in Templates or Folders

The following tasks show you how to add, change, and remove an operating system for templates or folders:

- Adding an Operating System to a Template

- Removing an Operating System from a Template
- Adding an Operating System to a Folder
- Removing an Operating System from a Folder

You cannot change or remove an operating system from a template or folder that is OS Independent.

Adding an Operating System to a Template

You cannot add an operating system to a template if the template inherits an operating system from a parent folder.

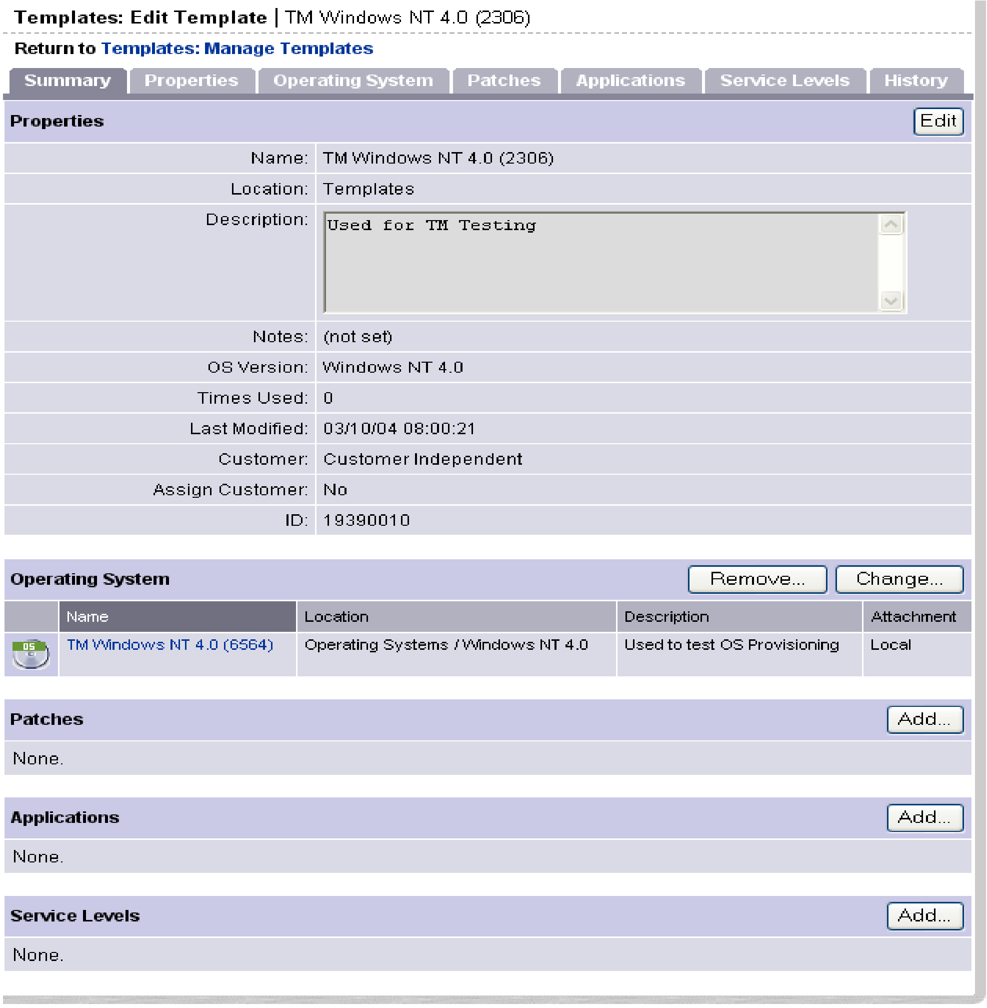
Perform the following steps to add an operating system to a template:

1. In the navigation panel of the Opsware Command Center, click Software ➤Templates. The Templates: Manage Templates page appears.

2 Select the template where you want to change the operating system. (If a template is inside another folder, you need to navigate to its location before you can select it.)

The Templates: Edit Template page appears, as Figure 10-26 shows.

Figure 10-26: Templates: Edit Template Page for Adding an Operating System to a Template



Templates: Edit Template | TM Windows NT 4.0 (2306)

Return to **Templates: Manage Templates**

Properties

Name:	TM Windows NT 4.0 (2306)
Location:	Templates
Description:	Used for TM Testing
Notes:	(not set)
OS Version:	Windows NT 4.0
Times Used:	0
Last Modified:	03/10/04 08:00:21
Customer:	Customer Independent
Assign Customer:	No
ID:	19390010

Operating System

	Name	Location	Description	Attachment
OS	TM Windows NT 4.0 (6564)	Operating Systems / Windows NT 4.0	Used to test OS Provisioning	Local

Patches

None.

Applications

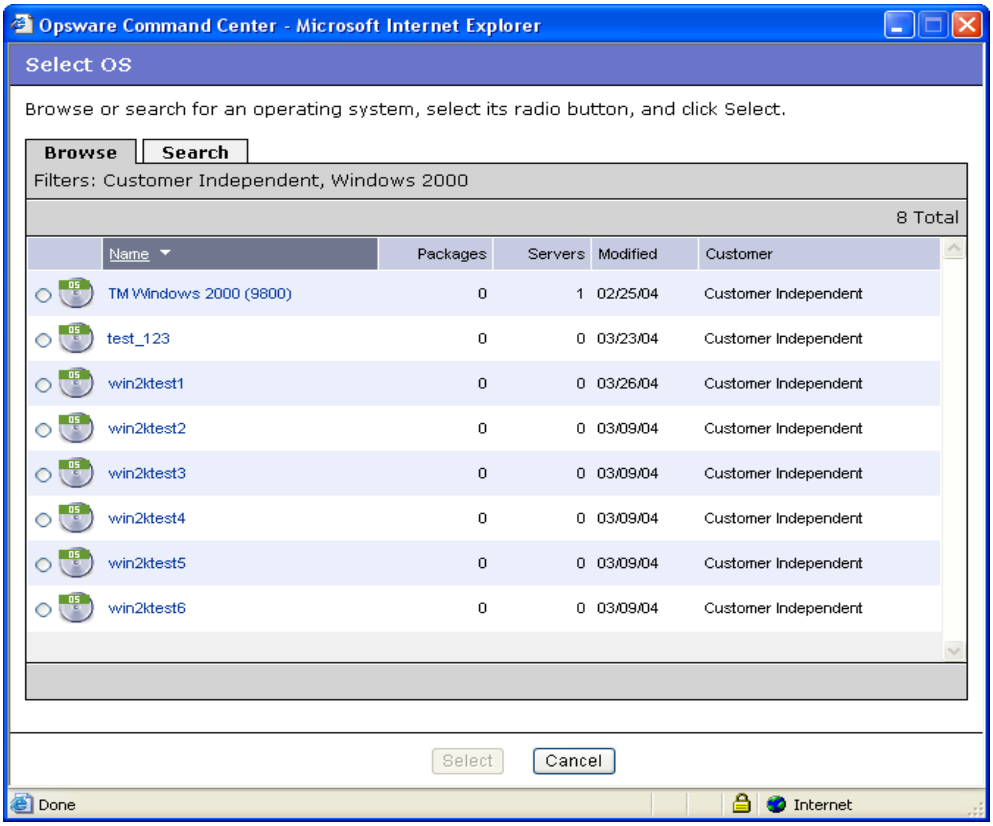
None.

Service Levels

None.

3 Click the Select button in the Operating System field. The Select OS window appears, as Figure 10-27 shows. (If the Template already has an operating system, click the Change button to change the operating system.)

Figure 10-27: Select OS Window



Browse or search for an operating system, select its radio button, and click Select.

Filters: Customer Independent, Windows 2000

8 Total

	Name	Packages	Servers	Modified	Customer
○	TM Windows 2000 (9800)	0	1	02/25/04	Customer Independent
○	test_123	0	0	03/23/04	Customer Independent
○	win2ktest1	0	0	03/26/04	Customer Independent
○	win2ktest2	0	0	03/09/04	Customer Independent
○	win2ktest3	0	0	03/09/04	Customer Independent
○	win2ktest4	0	0	03/09/04	Customer Independent
○	win2ktest5	0	0	03/09/04	Customer Independent
○	win2ktest6	0	0	03/09/04	Customer Independent

4 Browse or search for the operating system that you want to add to the template and select it by clicking its radio button.

5 Click the Select button to add or change the operating system.

Removing an Operating System from a Template

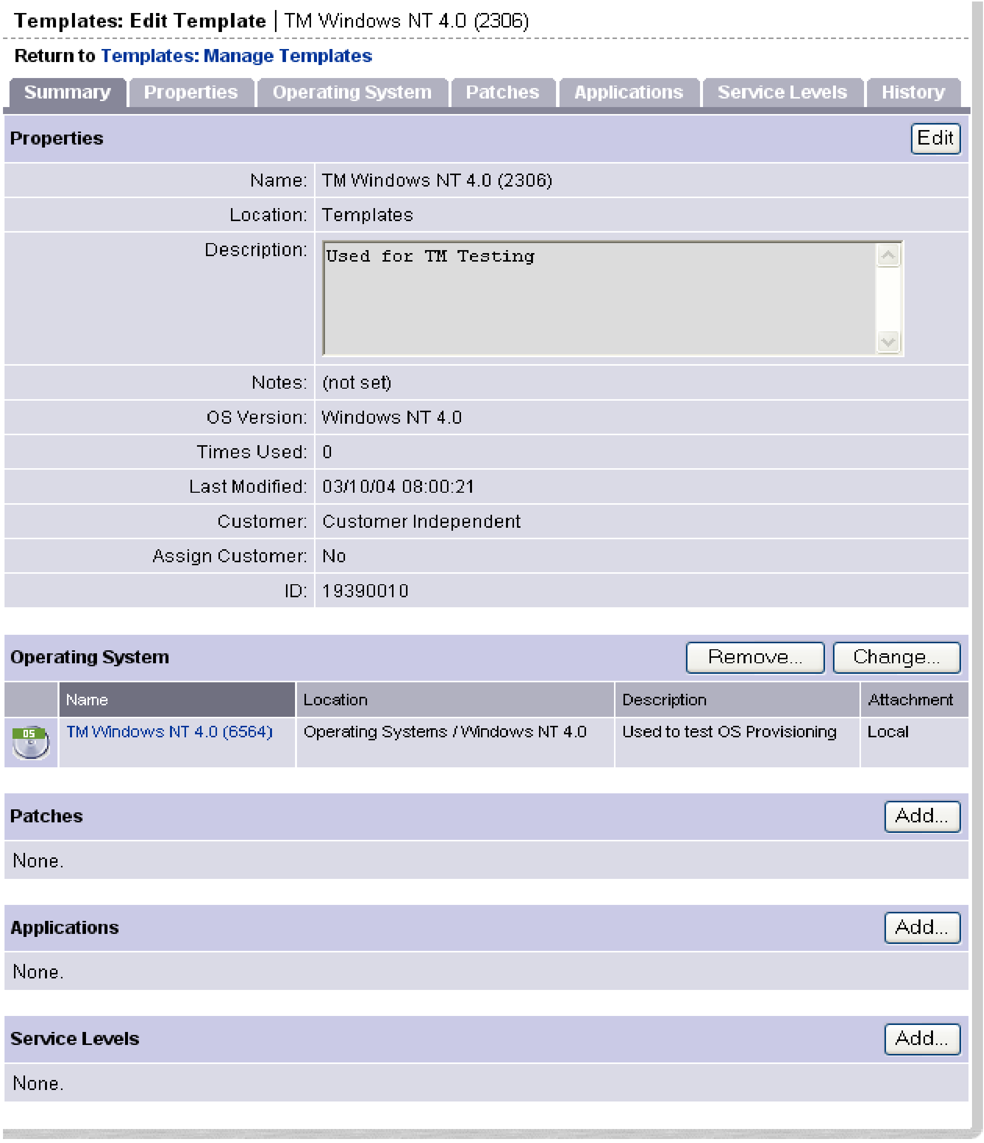
If the template inherits an operating system from a parent folder, then you cannot remove an operating system from the template.

Perform the following steps to remove an operating system from a template:

1 In the navigation panel of the Opsware Command Center, click Software and then click Templates. The Templates: Manage Templates page appears.

2 Select the template where you want to change the operating system. (If a template is inside another folder, you need to navigate to its location.) The Edit Templates page appears, as Figure 10-28 shows.

Figure 10-28: Templates: Edit Template Page for Removing an Operating System from a Template



Templates: Edit Template | TM Windows NT 4.0 (2306)

Return to Templates: Manage Templates

Properties

Name:	TM Windows NT 4.0 (2306)
Location:	Templates
Description:	Used for TM Testing
Notes:	(not set)
OS Version:	Windows NT 4.0
Times Used:	0
Last Modified:	03/10/04 08:00:21
Customer:	Customer Independent
Assign Customer:	No
ID:	19390010

Operating System

	Name	Location	Description	Attachment
OS	TM Windows NT 4.0 (6564)	Operating Systems / Windows NT 4.0	Used to test OS Provisioning	Local

Patches

None.

Applications

None.

Service Levels

None.

3 In the Operating System field, click the Remove button.

4 You are asked to confirm that you want to remove the operating system from the template. Click Yes to remove the operating system from the template.

Adding an Operating System to a Folder

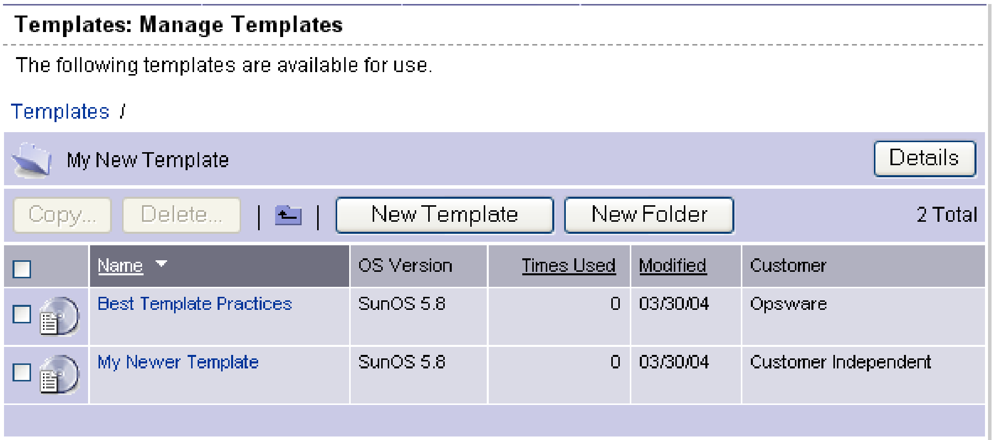
You cannot add an operating system to a folder that has any children that already have an operating system, or that inherits an operating system from a parent folder.

Perform the following steps to add an operating system to a folder:

1. In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

2. Select the folder where you want to change the operating system. (If the folder is inside another folder, you need to navigate to its location before you can select it.) The folder contents appear, as Figure 10-29 shows.

Figure 10-29: Folder Contents



Templates: Manage Templates

The following templates are available for use.

Templates /

My New Template

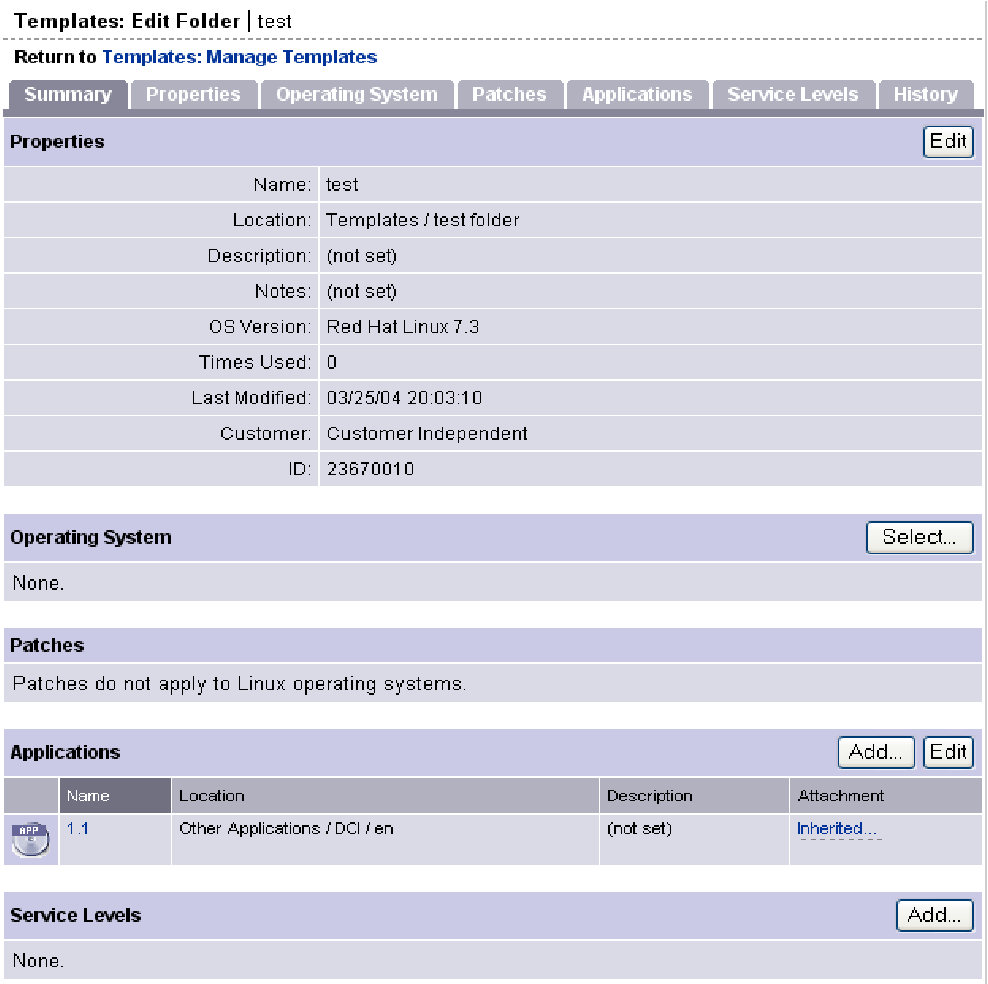
2 Total

□	Name	OS Version	Times Used	Modified	Customer
□	Best Template Practices	SunOS 5.8	0	03/30/04	Opsware
□	My Newer Template	SunOS 5.8	0	03/30/04	Customer Independent

3. Click the Details button. The folder's property summary page appears, as Figure 10-30 shows.

The Details button is only available when the folder has no children that have an operating system or does not inherit an operating system from a parent folder.

Figure 10-30: Folder Properties



Templates: Edit Folder | test

Return to Templates: Manage Templates

Properties

Name:	test
Location:	Templates / test folder
Description:	(not set)
Notes:	(not set)
OS Version:	Red Hat Linux 7.3
Times Used:	0
Last Modified:	03/25/04 20:03:10
Customer:	Customer Independent
ID:	23670010

Operating System

None.

Patches

Patches do not apply to Linux operating systems.

Applications

	Name	Location	Description	Attachment
APP	1.1	Other Applications / DCI / en	(not set)	Inherited...

Service Levels

None.

4 To add an operating system, from the Operating System section, click the Select button.

5 In the Select OS Window, browse or search for the operating system that you want to install and select it by clicking its radio button.

6 Click the Select button to add the operating system to the folder.

Removing an Operating System from a Folder

You cannot remove an operating system from a folder if the operating system is inherited from the parent.

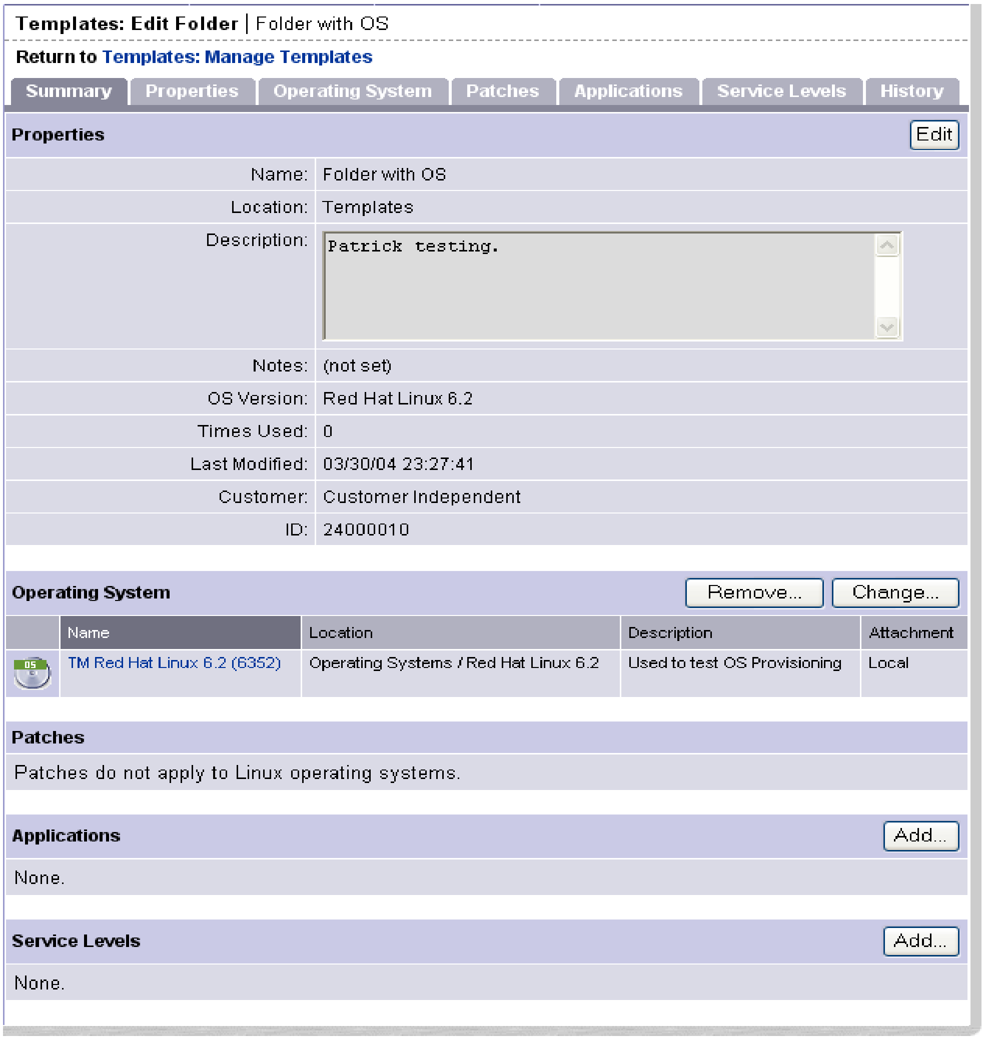
When you remove an operating system from a folder, the folder no longer appears in the Install OS Wizard when you use a template to install an operating system on a server.

Perform the following steps to remove an operating system from a folder:

1. In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.
2. Select the folder where you want to remove an operating system. (If the folder is inside another folder, you need to navigate to its location before you can select it.)
3. In the Folder Contents page, click the Details button.

4 In the Summary page for the selected folder, in the Operating System field, click the Remove button, as Figure 10-31 shows.

Figure 10-31: Remove Operating System from a Folder



Templates: Edit Folder | Folder with OS

Return to Templates: Manage Templates

Properties

Name:	Folder with OS
Location:	Templates
Description:	Patrick testing.
Notes:	(not set)
OS Version:	Red Hat Linux 6.2
Times Used:	0
Last Modified:	03/30/04 23:27:41
Customer:	Customer Independent
ID:	24000010

Operating System

	Name	Location	Description	Attachment
OS	TM Red Hat Linux 6.2 (6352)	Operating Systems / Red Hat Linux 6.2	Used to test OS Provisioning	Local

Patches

Patches do not apply to Linux operating systems.

Applications

None.

Service Levels

None.

5 You are asked to confirm that you want to remove the operating system from the folder. Click Yes to remove the operating system from the folder.

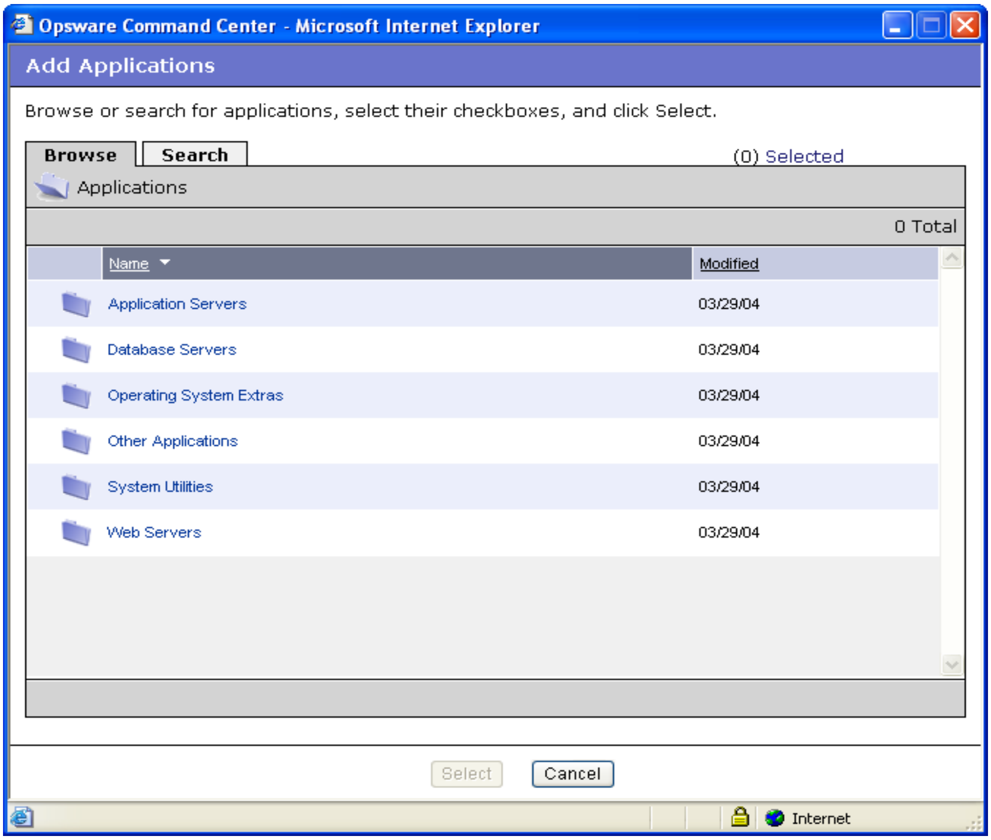
If you remove an operating system from a folder that has child folders, you are not able to add another operating system at the same level. Instead, use the Change button in the Operating System field.

Adding Applications to Templates or Folders

Perform the following steps to add an application to a template or to a folder:

1. From the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.
2. Select the template or folder where you want to add an application. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.)
3. If you are adding an application to a folder, click the Details button. If you are adding an application to a template, go to the next step.
4. To include applications in your template, click the Add button in the applications field. The Add Applications page appears, as Figure 10-32 shows.

Figure 10-32: Add Applications Page



Opsware Command Center - Microsoft Internet Explorer

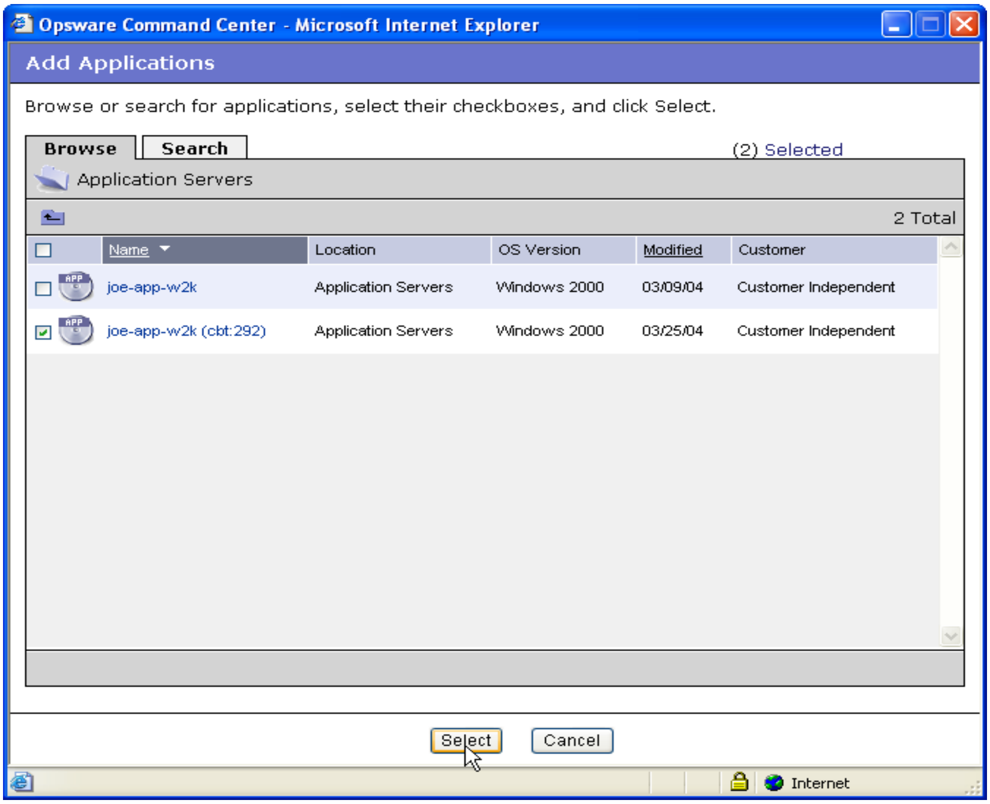
Add Applications

Browse or search for applications, select their checkboxes, and click Select.

Name	Modified
Application Servers	03/29/04
Database Servers	03/29/04
Operating System Extras	03/29/04
Other Applications	03/29/04
System Utilities	03/29/04
Web Servers	03/29/04

5 Browse or search for the applications that you want to add. Select the applications by clicking their checkboxes, and then click the Select button to add them to your template or folder, as Figure 10-33 shows.

Figure 10-33: Adding Applications to a Template



Opsware Command Center - Microsoft Internet Explorer

Add Applications

Browse or search for applications, select their checkboxes, and click Select.

Browse | Search — (2) Selected

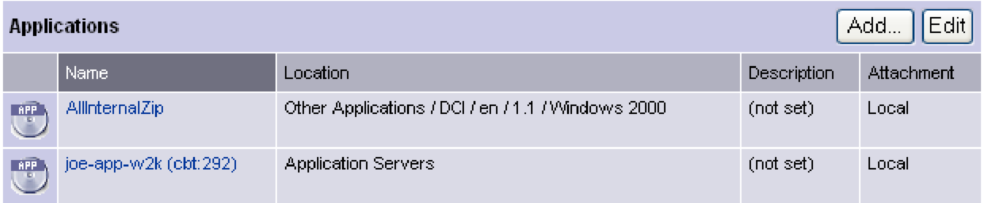
Application Servers

2 Total

□	Name	Location	OS Version	Modified	Customer
□	joe-app-w2k	Application Servers	Windows 2000	03/09/04	Customer Independent
☑	joe-app-w2k (cbt:292)	Application Servers	Windows 2000	03/25/04	Customer Independent

6 When you add the application to the template or folder, it shows in the Applications field of the Edit Template page, as Figure 10-34 shows.

Figure 10-34: Applications Added to a Template



Applications

	Name	Location	Description	Attachment
APP	AllInternalZip	Other Applications / DCI / en / 1.1 / Windows 2000	(not set)	Local
APP	joe-app-w2k (cbt:292)	Application Servers	(not set)	Local

Editing or Removing Applications for Templates or Folders

Perform the following steps to edit or to remove applications:

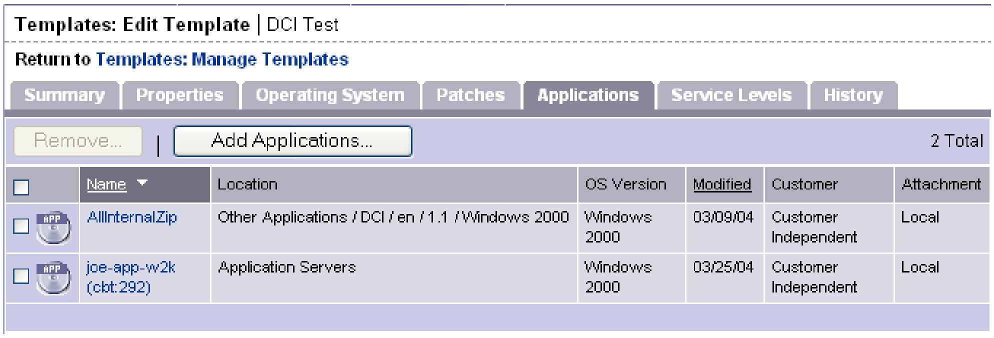
1. In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

2. Select the folder or template where you want to edit an application. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.)

3. If you are adding an application to a folder, click the Details button. If you are adding an application to a template, go to the next step.

4. Click the Edit button in the Applications field. The Templates: Edit Template page appears with the Applications tab active, as Figure 10-35 shows.

Figure 10-35: Edit Applications Page



Templates: Edit Template | DCI Test

Return to Templates: Manage Templates

2 Total

☐	Name ▼	Location	OS Version	Modified	Customer	Attachment
☐	AllInternalZip	Other Applications / DCI / en / 1.1 / Windows 2000	Windows 2000	03/09/04	Customer Independent	Local
☐	joe-app-w2k (cbt:292)	Application Servers	Windows 2000	03/25/04	Customer Independent	Local

5. To remove applications, click the checkbox next to the name of the application that you want to remove.

Inherited and blocked applications do not have a selectable checkbox so you cannot remove them here. You have to remove them from the folder where they are attached locally.

6. Click the Remove button.

7. The Remove Applications confirmation page appears. Click the Remove button to remove the applications.

8 You are asked to confirm that you want to remove the selected application. Click Yes to remove the application.

Adding Patches to Templates or Folders

In the Patches area of the Edit Template page, you have the option of either adding or editing patches. If you choose to edit patch attachments, you can both remove existing patches and add new patches.

Perform the following steps to add patches to a template or a folder:

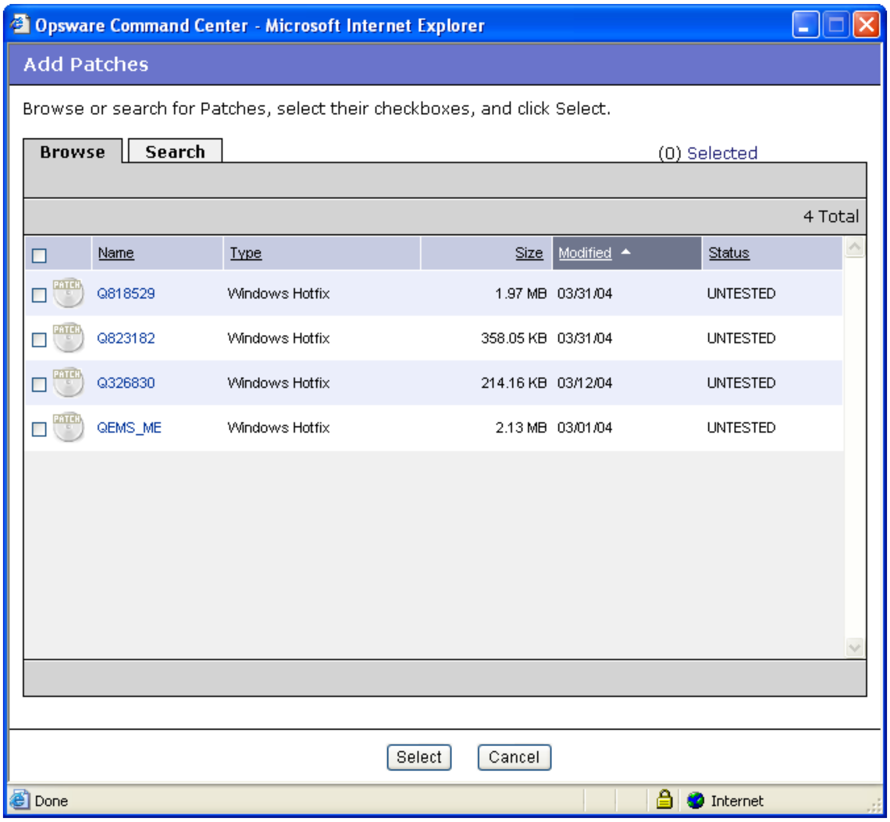
1 In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

2 Select the folder or template where you want to add a patch. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.)

3 If you are adding a patch to a folder, click the Details button. If you are adding a patch to a template, go to the next step.

4 Click the Add button in the Patches field. The Add Patches window appears, as Figure 10-36 shows.

Figure 10-36: Add Patches Window



Browse or search for Patches, select their checkboxes, and click Select.

(0) Selected

4 Total

□	Name	Type	Size	Modified ▲	Status
□	Q818529	Windows Hotfix	1.97 MB	03/31/04	UNTESTED
□	Q823182	Windows Hotfix	358.05 KB	03/31/04	UNTESTED
□	Q326830	Windows Hotfix	214.16 KB	03/12/04	UNTESTED
□	QEMS_ME	Windows Hotfix	2.13 MB	03/01/04	UNTESTED

5 Browse or search for the patches that you want to add to the template or folder. Click the checkboxes for the desired patches and then click the Select button to add the patches.

Editing or Removing Patches for Templates or Folders

In the Patches area of the Edit Template page, you have the option of either adding or editing patch attachments. If you choose to edit patch attachments, you can remove existing patches *and* add new patches.

Perform the following steps to edit or remove patches:

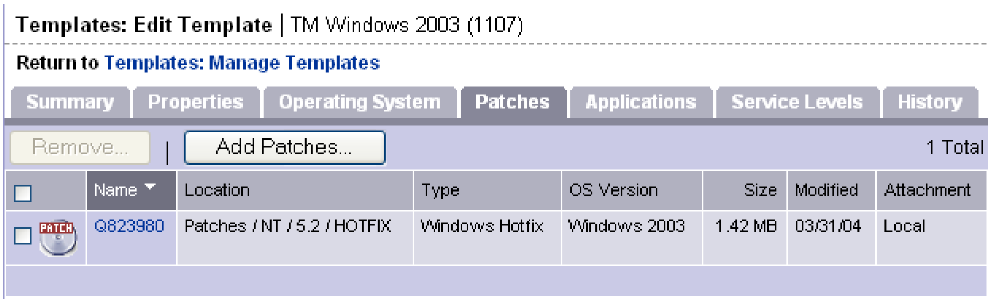
1 In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

2 Select the folder or template where you want to edit a patch. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.)

3 If you are editing the patch of a folder, click the Details button. If you are adding a patch to a template or folder, go to the next step.

4 Click the Edit button in the Patches field. The Templates: Edit Template page appears with the Add Patches tab active, as Figure 10-37 shows.

Figure 10-37: Templates: Edit Template Page - Edit Patches



Templates: Edit Template | TM Windows 2003 (1107)

Return to Templates: Manage Templates

□	Name ▾	Location	Type	OS Version	Size	Modified	Attachment
□ PATCH	Q823980	Patches / NT / 5.2 / HOTFIX	Windows Hotfix	Windows 2003	1.42 MB	03/31/04	Local

5 To remove patches, click the checkbox next to the name of the patches that you want to remove.

Inherited and blocked patches do not have a selectable checkbox so you cannot remove them here. You must remove them from the folder where they are attached locally.

6 Click the Remove button

7 The Remove Patches confirmation page appears. Click the Remove button to remove the patches from the template or folder.

8 To add patches to the template or folder, click the Add button. The Add Patches page appears.

9 Browse or search for the patches that you want to add. Select them by clicking their checkboxes and then click the Select button.

Adding Service Levels in Templates or Folders

Perform the following steps to add service levels in templates or folders:

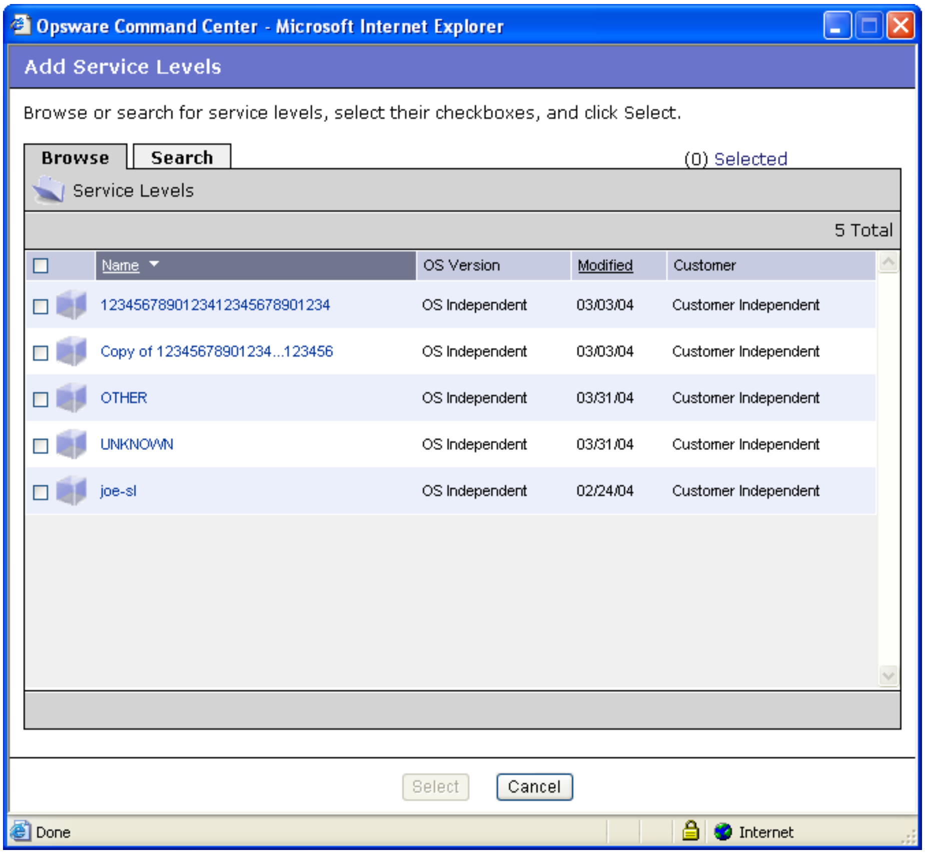
1. In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

2. Select the template or folder where you want to add a service level. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.)

3. If you are adding a service level to a folder, click the Details button. If you are adding a service level to a template, move to the next step.

4. Click the Add button in the Service Levels field. The Add Service Levels page appears, as Figure 10-38 shows.

Figure 10-38: Add Service Levels Page



Opsware Command Center - Microsoft Internet Explorer

Add Service Levels

Browse or search for service levels, select their checkboxes, and click Select.

□	Name	OS Version	Modified	Customer
□	123456789012341234567890l234	OS Independent	03/03/04	Customer Independent
□	Copy of 12345678901234...123456	OS Independent	03/03/04	Customer Independent
□	OTHER	OS Independent	03/31/04	Customer Independent
□	UNKNOWN	OS Independent	03/31/04	Customer Independent
□	joe-sl	OS Independent	02/24/04	Customer Independent

5 Browse or search for the service levels that you want to include in your template. Select the service levels by clicking the checkboxes, and then click the Select button to add them to your template or folder.

See the *Opsware® SAS 5.2 User's Guide* for more information about Service Levels.

Editing or Removing Service Levels in Templates or Folders

Perform the following steps to edit or remove service levels in templates or folders:

1 Click the Edit button in the Service Levels field. The Edit Template page appears with the Service Levels tab active.

2 To remove service levels, click the checkbox next to the name of the service levels that you want to remove.

Inherited and blocked service levels do not have a selectable checkbox so you cannot removed them from here. You have to remove them from the folder where they are attached locally.

3 Click the Remove button.

4 The Remove Service Levels confirmation page appears. Click the Yes button to remove the service levels from the template or folder.

Copying Templates and Folders

You can copy a template or a folder as a convenient way to use existing folders or templates without having to re-create a template or an entire hierarchy of folders.

When you copy a template, the copy has the same attachments as the original template. If the original template has attachments inherited from an ancestor folder, the copy also has all the ancestor folders and the local attachments that were inherited by the template.

When you copy a folder, the copy has the same attachments and the same children with all of the attachments as the original folder.

Perform the following steps to copy a template or a folder:

1 In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

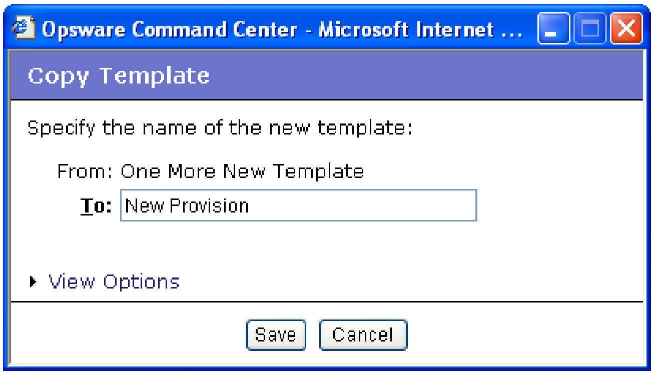
2 Select the folder or template that you want to copy. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.)

3 If you are copying a folder, click the Details button. If you are copying a template, move to the next step.

4 Click the Copy button.

5 In the Copy Template/Folders window, enter the name that you want to apply to the copied folder or template or accept the default, as Figure 10-39 shows.

Figure 10-39: Copy Template Window



Opsware Command Center - Microsoft Internet ...

Copy Template

Specify the name of the new template:

From: One More New Template

To: New Provision

The default option is to copy a folder as another folder and a template as a template.

6 You have the option of clicking the View Options link to show the Copy as Folder or Copy as Template options.

If you copy a folder that already has children, and you would like to make a copy of the folder and all its children, make sure you copy as a folder. If you copy a template or a folder as a template, it is unable to have children.

7 Click the Save button. The new folder or template now appears on the list of templates.

Deleting Templates or Folders

Perform the following steps to delete a template or a folder:

1 In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.

2. Select the folder or template that you want to delete. (If a template or folder is inside another folder, you need to navigate to its location before you can select it.) Selecting a folder or template activates the Copy and Delete buttons.
3. Click the Delete button.
4. You are asked to confirm that you want to delete the folder. Click Yes to complete the deletion, or No to cancel. The deleted folder or template is removed from the list of templates.

Blocking Folders and Templates from Inheriting

Making a change to an attachment at the top level of a template hierarchy results in a change to all the children of that top-level folder, unless a child folder has already had the attachment blocked.

You can only block inherited attachments. The equivalent for a local attachment is to delete it.

Blocking vs. Removing Attachments

The following list describes some issues to think about when you are deciding to block or remove an attachment from a folder or template:

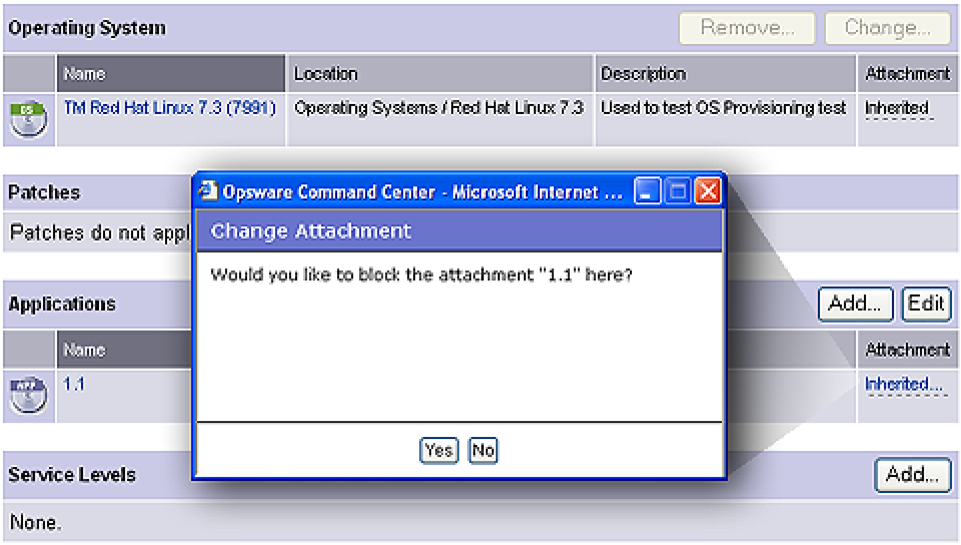
- You have the option of blocking attachments and preventing inheritance from a parent folder.
- You have the option of removing local attachments.
- Block an attachment when you do not want it to be inherited at the current level or at any subsequent levels of the hierarchy.
- Remove a local attachment when you do not want it to be in your hierarchy at all, or if you plan to attach a different version of the node. If you plan to attach a different version, remove the old version first to avoid conflicts.
- If you remove an attachment, any blocks to that attachment remain in the hierarchy until you remove them. These blocks continue to appear, but when you move your mouse over them you see that they are inactive. If you click an inactive block, a window appears asking if you want to delete the block. Click Yes to remove it.

To Block an Attachment from Being Inherited

Perform the following steps to block an attachment from being inherited:

1. In the navigation panel of the Opsware Command Center, click Software ➤ Templates. The Templates: Manage Templates page appears.
2. Navigate to the folder whose attachment you want to block.
3. Locate the operating system, patch, application, or service level attachment that you want to block.
4. Click the link that says Inherited. It changes to Blocked. Click it again to change it to Inherited if you want to remove the block, as Figure 10-40 shows.

Figure 10-40: Blocking Inherited Attachment



Operating System

	Name	Location	Description	Attachment
	TM Red Hat Linux 7.3 (7991)	Operating Systems / Red Hat Linux 7.3	Used to test OS Provisioning test	Inherited

Patches

Patches do not appl

Applications

	Name	Attachment
	1.1	Inherited...

Service Levels

None.

Change Attachment

Would you like to block the attachment "1.1" here?

5. To remove the block, click the link named Blocked. A dialog box allows you to change it back to Inherited.

]

Chapter 11: Patch Management Setup

IN THIS CHAPTER

This chapter discusses the following topics:

- Opsware Patch Management
- Patch Management for Each Operating System
- Patch Management Roles
- Uploading Patches
- Patch Administration Using the Opsware Command Center

Opsware Patch Management

This section provides information about patch management within Opsware SAS and contains the following topics:

- Overview of Patch Management
- Summary of Features for Patch Management
- How Opsware SAS Supports Patch Management
- Support for Patch Testing and Installation Standardization

Overview of Patch Management

Opsware SAS automates the key aspects of patch management, while offering a fine degree of control over how and under what conditions patches are installed.

Because patches are often released to address grave security threats, an organization needs to be able to roll out patches quickly, before systems become compromised. At the same time, however, patches can cause serious problems, from performance degradation to server failures.

The Patch Management feature allows you to react quickly to newly discovered threats, but it also provides support for strict testing and standardization of patch installation. And, if patches later cause problems even after being tested and approved, the Patch Management feature also allows you to uninstall the patches in a safe and standardized way.

Patch management is a fully integrated component of Opsware SAS, and leverages Opsware SAS' complement of server automation features. Opsware SAS, for example, maintains a central database (called the Model Repository) that has detailed information about every server under management, the patches and software installed on the servers, and the patches and software available for installation. You can use this data to determine the severity of your exposure to a newly discovered threat, and to help you assess the benefits of rolling out a patch versus the costs in downtime and testing requirements.

By automating the patching procedure, the Patch Management feature can reduce the amount of downtime required for patching. Opsware SAS also allows you to schedule patch activity, so that patching occurs during off-peak hours.

After the patch is integrated into your environment, you can make it part of your standard builds with Opsware templates.

Summary of Features for Patch Management

Opsware SAS automates patch management by providing the following features:

- A central repository where patches are stored and organized in their native formats
- A database that includes information on every patch that has been applied
- Customized scripts that can be run before and after a patch is installed
- Microsoft servers are analyzed against a Microsoft database to determine which servers need which patches
- Advanced search abilities to identify servers that require patching
- Auditing abilities so that security personnel can track the deployment of important patches

How Opsware SAS Supports Patch Management

When a server is brought under management by Opsware SAS, the Opsware Agent installed on the server registers the server's hardware and software configuration with Opsware SAS. (The Opsware Agent repeats this registration every twenty-four hours.) This information, which includes data about the exact OS version, hardware type, installed software and patches, is immediately recorded in the Model Repository. Also, when you first provision a server with Opsware SAS, the same data is immediately recorded.

When a new patch is issued, you can use the Opsware Command Center to immediately identify which servers require patching. Opsware SAS provides a Software Repository where you upload patches and other software. Users access this software from the Opsware Command Center to install patches on the appropriate servers.

After a server is brought under management, you should install all patches by using the Patch Management feature. If you install a patch manually, Opsware SAS does not have data about that patch until the next software registration. If you install a patch manually, it can take as long as twenty-four hours until the data about that server in the Model Repository is up-to-date.

Whenever you install or uninstall software or patches with Opsware SAS, however, the Opsware Agent immediately updates the information about the server in the Model Repository.

Support for Patch Testing and Installation Standardization

Opsware SAS offers features to minimize the risk of rolling out patches. First, when a patch is uploaded into Opsware SAS, its status is marked as *untested* and only administrators with special privileges can install it.

The patch administrator then defines patch installation and uninstallation options and tests the patch. Only after the patch is tested and the patch administrator marks it as *available* for use can other administrators install the patch.

The Patch Management feature allows you to standardize the way that patches are installed and uninstalled, thereby preventing ad-hoc installation procedures. Patch administrators standardize patch installation by providing pre- and post-install scripts, install and uninstall flags, and instructions on when to reboot and how to handle error codes from the pre- and post-install scripts.

Patch Management for Each Operating System

This section discusses the following topics:

- Summary of Features for Patch Management
- Supporting Technologies for Patch Management

- Special Support for Windows Servers
- About Windows Patches
- About AIX Patches
- About Solaris Patches
- About HP-UX Patches
- Overview of Installation Scripts
- Overview of Installation and Uninstallation Flags

Supported Operating Systems and Supported Patch Types

The Patch Management feature supports all of the operating system versions that Opsware SAS supports, except for Linux.

Linux does not support patches in the ordinary sense. The packages are not patchable. Instead, new versions of the RPM are delivered. Linux systems that Opsware SAS manages are therefore not viewable through the Patch Management feature interfaces. New Linux packages and updates should be managed and applied though the software page.

The following table shows the operating system versions and the patch types that the Patch Management feature supports.

Table 11-1: Supported Operating System Versions and Patch Types

OS VERSIONS	PATCH TYPES
AIX 4.3	AIX Update Fileset APARs
AIX 5.1	AIX Update Fileset APARs
AIX 5.3	AIX Update Fileset APARs
HP-UX 11.00	HP-UX Patch Filseset HP-UX Patch Products

Table 11-1: Supported Operating System Versions and Patch Types

OS VERSIONS	PATCH TYPES
Solaris 6	Solaris Patch Solaris Patch Cluster
Solaris 7	Solaris Patch Solaris Patch Cluster
Solaris 8	Solaris Patch Solaris Patch Cluster
Solaris 9	Solaris Patch Solaris Patch Cluster
Solaris 10	Solaris Patch Solaris Patch Cluster
Windows NT 4.0	Windows Hotfix Windows OS Service Pack
Windows 2000	Windows Hotfix Windows OS Service Pack
Windows 2003	Windows Hotfix Windows OS Service Pack

Supporting Technologies for Patch Management

The Patch Management feature uses patching utilities and technologies for each supported operating system. Opsware SAS uses these tools behind the scenes, which allows you to perform patch management though a single interface, without having to worry about invoking a number of different patching utilities.

Opsware SAS models the way it treats patches on the way the underlying utility treats a patch. For example, if the Solaris patchadd utility is not able to install one patch contained in a patch cluster, the Solaris utility continues to install the remaining patches in the patch cluster. Opsware SAS respects this behavior and allows that patch installation operation to continue. Any patches that are not installed are reported at the end of the installation operation.

The following table shows the patch management and installation tools that are used for each of the supported operating systems.

Table 11-2: Supporting Technologies for Patch Management

WINDOWS	SOLARIS	AIX	HU-UX
Qchain enables single reboot when installing more than one Hotfix	Patchadd installs Solaris patches	Installp installs and uninstalls filesets	Swlist lists patch products, files, products, and filesets
mbsacli lists and verifies installed Hotfixes and Service Packs	Patchrm uninstalls Solaris patches	Lslpp lists installed LPPs	Swinstall installs a depot
	Showrev lists installed Solaris patches	Instfix lists installed APARs	Swremove removes a depot
	Pkgadd installs Solaris packages		
	Pkginfo lists installed Solaris packages		

Special Support for Windows Servers

The Patch Management feature offers an even higher degree of patch automation for Windows servers. Opsware SAS takes advantage of the Microsoft Patch Database, which contains information about what patches are available and how the patches should be applied. Opsware SAS compares all Windows servers to this database, which allows the patch administrator to determine which patches need to be applied. When the Microsoft

Patch Database is updated, the new patches that have not yet been uploaded display in the Opsware Command Center, with links to the patches that allow the patch administrator to immediately download the patches.

About Windows Patches

You can download most Windows patches from Microsoft directly though the Opsware Command Center. All of the Windows patches that affect any of the Microsoft products that Opsware SAS is configured to track appear in the Patch Management pages. If the patch is new and has not yet been uploaded, a link to the patch on the Microsoft support site is provided in the Opsware Command Center that you can use to immediately download the patch.

After you download the Windows patch, however, you must still upload the patch through the Upload Patch Wizard or the OCLI.

If a Windows patch is already uploaded and installed on a server, for example, as part of an Opsware template, you receive a warning that the patch is already uploaded:

```
This patch already exists within Opsware SAS and is utilized by
node(s). The following entries are the optional settings for
patch installation.
```

As with all patch types, you must be careful to specify the correct type of patch you are uploading, such as a Windows Hotfix or Windows OS Service Pack. Misidentifying Windows patches can cause additional problems because the information you provide about the patch conflicts with the data in the Microsoft Patch Database.

The Patch Management feature passes in install or uninstall flags that cause Windows patches to install and uninstall in *silent* mode, meaning that no dialog boxes should appear on the server while installing or uninstalling a patch. Some Windows patches, however, still produce modal dialog boxes when they are being installed or uninstalled, even when directed not to do so. Opsware SAS has a special utility that automatically closes these modal dialog boxes.

Microsoft Patch Management Prerequisites

You must have Internet Explorer 5.0.1 or later installed on the server in order to use its native Microsoft Baseline Security Analyzer (MBSA) tool. Opsware SAS uses the MBSA tool for patch management.

You must also have an XML parser such as MSXML version 3.0 SP2 installed in order for the tool to function correctly.

Windows NT Service Pack 6a must be installed in order to add Microsoft Installer support to Windows NT.

About AIX Patches

AIX periodically releases Authorized Program Analysis Reports (APARs), which specify what update filesets (contained in LPPs) are necessary to fix an identified problem. An APAR only specifies the minimum version of an update fileset required to fix a problem; an APAR can therefore be satisfied with later versions of the same filesets. To maintain compatibility, however, Opsware SAS always adopts the fileset with the lowest version number that meets the minimum version that APAR specifies. If a later version of the update fileset is uploaded, Opsware SAS still associates the earlier version of the fileset with the APAR.

When an LPP is uploaded into Opsware SAS, Opsware recognizes which APARs the filesets contained in the LPP belong to. An entry is created for the APAR in the Patch Management feature when the first fileset associated with an APAR is uploaded. (In some cases, a fileset is associated with more than one APAR. An entry is created for each APAR the fileset is associated with, if the entry does not already exist.)

If you want to be able to install all LPPs that APAR specifies, you must make certain to upload all of the specified LPPs into the Patch Management feature, either through the Upload Patch Wizard or through the OCLI.

If you do not upload all of the LPPs that APAR specifies, it is still possible for the system administrator to browse for an APAR and install the partial set of LPPs that are uploaded. In such cases, the administrator receives a warning that the filesets for the APAR are not all installed.

The Patch Administrator must first upload and test an LPP before it is generally available in Opsware SAS. The new fileset is integrated into the APAR only after the LPP is tested and approved. Even though the APAR is updated automatically, you still maintain control over the exact filesets that are allowed to be installed on your managed servers.

APAR update filesets cannot be installed on a server if the server does not already have the base filesets for which the update filesets are intended.

If, however, a server has a partial set of the base filesets, the APAR can be applied and only the applicable filesets for the base filesets are installed. For example, if an APAR specifies four update filesets to update four base filesets, and you attempt to apply the APAR to a server that has only three of the base filesets, three of the four update filesets from the APAR are installed.

About Solaris Patches

A Solaris patch cluster contains a set of selected patches for a specific Solaris release level. Ordinarily, after a patch cluster is installed, it is not possible to search for a particular patch cluster. The patches do not contain any metadata that relate them to the patch cluster in which they were originally bundled. You can only search for the individual patches.

If you install a Solaris patch cluster by using the Patch Management feature, however, Opsware SAS keeps track of the patch cluster in the Model Repository. You can therefore search for a patch cluster to determine if a full patch cluster is installed. You can also uninstall the patch cluster if you installed it with the Patch Management feature.

About HP-UX Patches

HP-UX patches are delivered exclusively as depots, which are patch products that contain patch filesets. The depot is uploaded directly into Opsware SAS by using the Patch Management feature.

If a depot is already uploaded and attached to a node, it cannot be uploaded by using the Patch Management feature. If you want to upload the depot by using the Patch Management feature, you must detach a depot from any nodes that it is attached to, and then delete it from the Software Repository.

For HP-UX 10.20, you can only apply patches through the Install Software Wizard because Opsware SAS recognizes them as software and not patches.

Overview of Installation Scripts

When you upload a patch, you can specify the following types of scripts:

- Pre-installation scripts that are executed before a patch is installed
- Post-installation scripts that are executed after a patch is installed
- Pre-uninstallation scripts that are executed before a patch is uninstalled

- Post-uninstallation scripts that are executed after a patch is uninstalled

A typical use of a pre-installation script is to shut down a process before you apply a patch to the application that the process belongs to. The post-installation script then restarts the process after the patch is applied.

A user can execute any kind of script that the operating system supports of the server where the patch is to be installed. You must make certain, however, that the proper shells, binaries, and so forth, are installed on the servers where you plan to run the scripts. For example, you can specify Python scripts to be run when the patch is installed, but you must make certain that Python is installed on the servers where you want to run the scripts. You must also call Python yourself. Opsware SAS does not call Python on your behalf.

Overview of Installation and Uninstallation Flags

You can specify installation and uninstallation flags that are applied whenever a patch is installed or uninstalled.

Opsware SAS, however, also uses default installation and uninstallation flags. Opsware SAS requires that patches are installed and uninstalled with these flags. You must therefore be certain that you do not specify any installation or uninstallation flags that override or contradict the default flags passed in by Opsware SAS.

Some Windows Hotfixes do not support the -z flag, some do not support the -q flag, and some do not support either. In such cases, you must use a special expression: /-z or /-q or /-z -q respectively, to prevent the Patch Management feature from passing in the -z or -q or -z -q flag.

Default Installation and Uninstallation Flags

The following table lists the default installation flags that Opsware SAS uses.

Table 11-3: Default Installation Flags

OPERATING SYSTEM/PATCH TYPES	FLAGS
Windows Hotfix	`-q -z`
Windows Security Rollup Package (treated identically to a Hotfix by the Patch Management feature)	`-q -z`

Table 11-3: Default Installation Flags

OPERATING SYSTEM/PATCH TYPES	FLAGS
Windows OS Service Pack	`-u -n -o -q -z`
AIX	`-a -Q -g -X -w`
HP-UX	None

The following table lists the default uninstallation flags that Opsware SAS uses.

Table 11-4: Default Uninstallation Flags

OPERATING SYSTEM/PATCH TYPES	FLAGS
Windows Hotfix	`-q -z`
Security Rollup Package	`-q -z`
Windows OS Service Pack	Not uninstallable
AIX	`-u -g -X`
AIX Reject Options	`-r -g -X`
HP-UX	None

Patch Management Roles

This section provides information on patch management roles and contains the following topics:

- Overview of Patch Management Roles
- About the Patch Administrator
- About the System Administrator

Overview of Patch Management Roles

Opsware SAS provides support for rigorous change management by assigning the functions of patch management to two different types of administrators:

- The patch administrator (often referred to as the security administrator), who has the authority to upload and test, and edit patch options

- The system administrator, who applies the patches (that have been approved for use) uniformly and automatically according to the options that the patch administrator specifies

Only the patch administrator should have the Patches permission, which gives access to advanced features not available through the Patch Management Wizards. Both administrators must have permissions for the Patch Management Wizards. To obtain these permissions, contact your Opsware administrator. For more information, see the Permissions Reference appendix in the *Opsware® SAS 5.2 Configuration Guide*.

About the Patch Administrator

In most organizations, patch administrators are responsible for reviewing the latest security threats and the patches that vendors have released to address these problems. The patch administrators are generally experts in the operating systems and applications that they manage, and are able to assess the necessity of applying patches issued by vendors. They are able to diagnose common problems that arise after patches are installed, allowing them to thoroughly test the patch application process.

In Opsware SAS, patch administrators are granted specific permissions that allow them to upload patches into Opsware SAS, test the patches, and then mark them as *available* for use. Basic users can upload patches, but they cannot install them or mark them as available. Patch administrators are also able to edit patch options (such as installation scripts) though patch management. Other types of users are not allowed to upload or edit patches.

Typically, the patch administrator uploads patches and then tests them on non-production reference hardware. After testing the patches and determining that the patches are safe to apply to production systems, they mark the patches available in the Opsware Command Center, and then advise the system administrators that they must apply the approved patches.

About the System Administrator

The Opsware users are system administrators who are responsible for the day-to-day maintenance of the servers in a deployment. These users are not required to have the same level of expertise in low-level system details as the patch administrator.

Because the patch administrator has set up the patch installation, the system administrators can apply the patches to a large number of servers with a few mouse clicks. They are responsible for searching for the servers that require the approved patch, running the Patch Installation Wizard, and verifying that the patches are installed successfully.

The system administrator cannot use the Patches link on the Opsware Command Center home page navigation panel. (This link requires the Patches permission.) The system administrator can upload patches through the Upload Patch Wizard, but cannot install a patch until the patch administrator has marked it as available. The system administrator can also uninstall patches and perform Microsoft patch updates.

Setting Up for Patch Management Feature

This section provides information about the set up for the patch management feature and contains the following topics:

- Overview of Setting Up for the Patch Management Feature
- About the Microsoft Patch Database
- Uploading the Microsoft Patch Database
- Products Tracked in the Microsoft Patch Database
- Selecting Which Microsoft Products to Track

Overview of Setting Up for the Patch Management Feature

Before you upload any patches, you should first upload the latest version of the mssecure.xml Microsoft Patch Database file if you have any Windows servers in your facility. The Patch Management feature also relies on two additional utilities, Qchain.exe and mbsacli.exe. These two utilities are uploaded when Opsware SAS is first installed. For additional requirements for Windows Servers to support patch management, see the *Opsware® SAS 5.2 Deployment and Installation Guide*.

About the Microsoft Patch Database

Once every twenty-four hours, the Opsware Agent on a Windows server compares the server's current state against the Microsoft Patch Database that has been uploaded into Opsware SAS by the patch administrator. The Opsware Agent reports the results of that comparison, and the data is stored in the Model Repository. When a user requests an analysis of a Windows server (for example, by using the Microsoft Patch Update Wizard), the data is retrieved from the Model Repository and displayed in the Opsware Command Center. By storing the data in the Model Repository, rather than performing an actual comparison on the server itself when a user requests an analysis, the data can be quickly retrieved and displayed.

If a user performs a patch analysis of a Windows server immediately after uploading a new version of the Microsoft Patch Database, the analysis does not yet include the data from the new patch database. Instead, Opsware SAS reports the data from the last time that the Opsware Agent recorded the results of its comparison.

About Uploading the Microsoft Patch Database

To upload the Microsoft Patch Database, you have two options. If your Opsware Command Center server has access to the Internet, you can specify the URL of the Microsoft Patch Database.

You must still re-upload from that URL when a new version of the database is released. The Microsoft Patch Database is generally updated once a month and you must re-upload the new version on a monthly basis.

If your Opsware Command Center is isolated from the Internet, you must periodically download the Microsoft XML database to a location on your network accessible to the Opsware Command Center and then upload it.

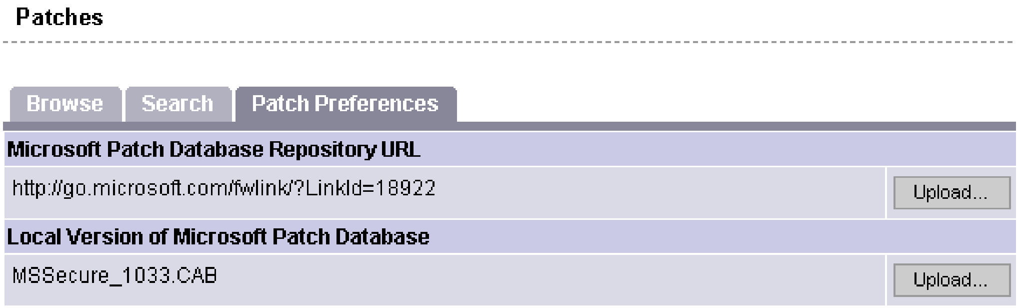
You can either upload the Microsoft Patch Database as a CAB archive, which contains an XML file, or you can upload the XML file directly. You can upload the patch database either with the Opsware Command Center or the Opsware Command Line Interface OCLI). See “OCLI 1.0 for Package Management” on page 227 in Chapter 8 for information about instructions on how to use the OCLI.

Uploading the Microsoft Patch Database

Perform the following steps to upload the Microsoft Patch Database:

1. From the navigation panel in the Opsware Command Center, click Software ➤ Patches. The Patches page appears.
2. Click the Patch Preferences tab. See Figure 11-1.

Figure 11-1: Patch Preferences Tab



Patches

Microsoft Patch Database Repository URL

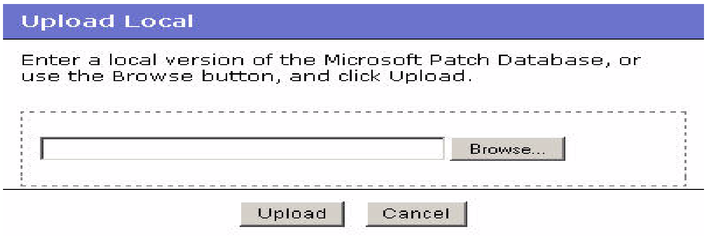
http://go.microsoft.com/fwlink/?LinkId=18922

Local Version of Microsoft Patch Database

MSSecure_1033.CAB

3. If you want to upload the mssecure.cab file from the Internet, click the Upload button under the Microsoft Patch Database Repository URL. The Upload URL page appears.
4. Specify the URL of the Microsoft Patch Database Repository URL and then click Upload.
5. If you do not want to upload the Microsoft Patch Database from the Internet, first copy the file to a location accessible to your Opsware Command Center server.
6. Specify the fully qualified path of the Microsoft Patch Database or click the Browse button and navigate to the database.
7. Click the Upload button. See Figure 11-2.

Figure 11-2: Upload Local Version of the Microsoft Patch Database



Upload Local

Enter a local version of the Microsoft Patch Database, or use the Browse button, and click Upload.

Products Tracked in the Microsoft Patch Database

The Microsoft Patch Database contains information about a wide range of Microsoft products. After you upload the database, you must select the products that you want to track. Opsware SAS tracks the data for the products that you select, and ignores information about the products that you do not use. If you do select products that you do not actually use, the patches for those products show up in the Opsware Command Center.

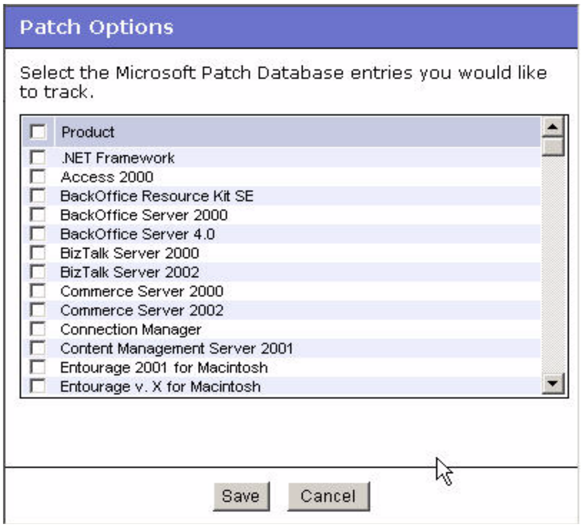
Selecting Which Microsoft Products to Track

Perform the following steps to select which Microsoft products to track:

1. From the navigation panel in the Opsware Command Center, click Patches ➤ Patch Preferences.

2. Under the Patch Options, click the Select button. The Patch Options page appears, as Figure 11-3 shows.

Figure 11-3: Microsoft Patch Options Page



Patch Options

Select the Microsoft Patch Database entries you would like to track.

□ Product
□ .NET Framework
□ Access 2000
□ BackOffice Resource Kit SE
□ BackOffice Server 2000
□ BackOffice Server 4.0
□ BizTalk Server 2000
□ BizTalk Server 2002
□ Commerce Server 2000
□ Commerce Server 2002
□ Connection Manager
□ Content Management Server 2001
□ Entourage 2001 for Macintosh
□ Entourage v. X for Macintosh

3. Click the check boxes for all of the Microsoft products whose Hotfixes you want to track.

4. Click Save. The next time the patch database is uploaded, Hotfixes that affect the set of selected products are modelled in Opsware SAS.

Uploading Patches

This section provides information about how to upload patches with Opsware SAS and contains the following topics:

- Overview of Uploading Patches
- Uploading Patches with Opsware Command Center or OCLI
- Preparing to Upload Patches
- Uploading a Patch with the Upload Patch Wizard
- About Testing Patches

Overview of Uploading Patches

When a patch is uploaded, you associate the patch with a specific version of an operating system. When you upload a Solaris patch, for example, you must select the version of the Solaris operating system that this patch applies to, such as Solaris 5.6 or 5.9. You can only install this patch on servers that are running that version of the operating system.

If, for any reason, you need to install a given patch across servers running different versions of the same operating system, you need to upload the patch multiple times and associate the patch with each of the operating system versions that the patch applies to.

For example, if the same Solaris patch needs to be installed on servers running Solaris 2.7 and 2.8, you must upload the patch two times. The first time that you upload the patch, you associate it with the Solaris 2.7. You then repeat the procedure and associate the patch with Solaris 2.8. (This procedure also allows you to specify different installation options. The different versions of the same operating system can sometimes require different installation scripts, installation flags, and so forth.)

In the case of application patches, it is even more common that you need to upload a patch multiple times. A Solaris patch for Oracle, for example, often needs to be applied to instances of Oracle running on slightly different versions of the Solaris operating system.

Uploading Patches with Opsware Command Center or OCLI

If you upload a patch though the Opsware Command Center, the Upload Patch Wizard guides you through the process. The Upload Patch Wizard allows you to specify a number of options for the patch, including install and post-install scripts, install and uninstall flags, and other options.

Because the Opsware Command Center is a browser-based interface, you can only upload one patch or patch container (such as a Solaris patch cluster or an HP-UX depot) at a time. If you want to upload multiple patches at the same time, such as a large set of AIX LPPs, you can do so more quickly through the OCLI.

If you upload patches through the OCLI, however, you are not able to specify installation options during the upload process. Instead, you specify these options by editing the patches through the Opsware Command Center.

Preparing to Upload Patches

Before you upload a patch, you must copy it to a location that is accessible to the browser that you are using or the OCLI. If you are using the Opsware Command Center, you specify the path of the patch in the upload wizard, either by entering it directly or by browsing for the patch.

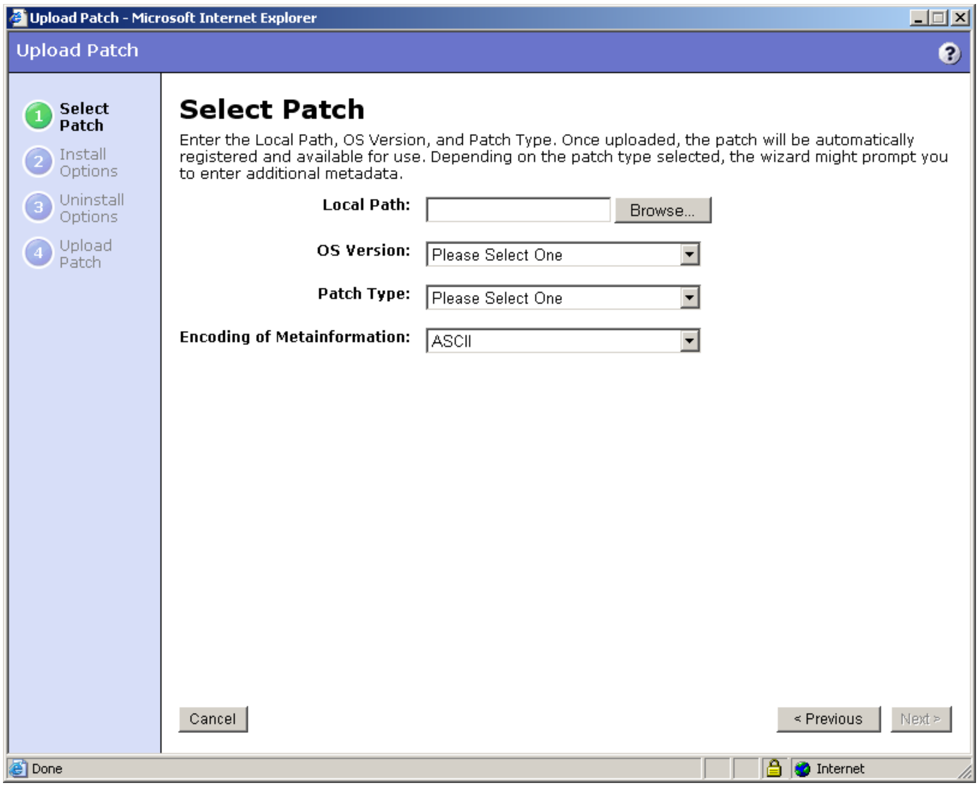
In some cases, you need to install patches in a particular order. You can create an installation order dependency by using the Opsware Command Center.

Uploading a Patch with the Upload Patch Wizard

Perform the following steps to upload a patch by using the Upload Patch Wizard:

1 Launch the Upload Patch Wizard from the Patch Management pane on the Opsware home page.The Select Patch page appears, as Figure 11-4 shows.

Figure 11-4: Select Patch Page



Select Patch

Enter the Local Path, OS Version, and Patch Type. Once uploaded, the patch will be automatically registered and available for use. Depending on the patch type selected, the wizard might prompt you to enter additional metadata.

Local Path:	
OS Version:	Please Select One
Patch Type:	Please Select One
Encoding of Metainformation:	ASCII

2 Either enter the fully qualified path of the patch that you want to upload, or click Browse and navigate to the patch that you want to upload.

3 Select the OS version of the patch that want to upload. You must be certain to select the correct operating version, or the patch will not be available for the correct operating system.

4 Select the type of patch that you are uploading. You must be careful to select the correct patch type or the patch will be misapplied, or uninstallable. The Opsware Command Center only allows you to select patches that are appropriate for the operating system that you select, but it is still possible to select the wrong kind of patch. (For example, selecting a Solaris patch when you intended to select a Solaris patch cluster.)

5 Click Next to continue to the Install Options page. In this page, you can specify a number of installation options:

- Install Flags passed directly to the patch installer. The Patch Management feature also passes a number of default flags.
  - If you are installing a Windows Hotfix that does not support the -z flag, remember to use the /-z option here to prevent the Patch Management feature from passing in the -z flag.
  - When installing an AIX Update fileset, the Patch Management feature normally applies the fileset, which allows it to be rejected (uninstalled.) If you want to commit the fileset instead (so that it cannot be removed), use the -c option here.
- Pre-install Script. Enter the pre-install script into this box.
- If you want to terminate the installation of the patch if the script returns a non-zero return code, select the check box.
- Post-Install Script: Enter the post-install script into this box. If you want to terminate the installation of the patch if the script returns a non-zero return code, select the check box.
- Select the Reboot on install option if the patch you are removing requires a reboot. Keep in mind that other patches can be directly applied after this patch, so be sure to check this option if it is necessary.

6 Click Next to continue to the Uninstall Options page.

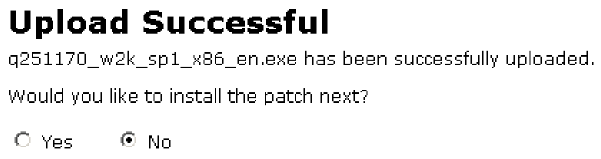
In this page, you can specify the following uninstallation options:

- Uninstall Flags passed directly to the installer. The Opsware Patch Management System passes a number of default uninstall flags to the installer.
- Pre-uninstall Script. Enter the Pre-uninstall script into this box.
- If you want to terminate the installation of the patch if the script returns a non-zero return code, select the check box.
- Post-uninstall Script: Enter the post-uninstall script into this box. If you want to terminate the installation of the patch if the script returns a non-zero return code, select the check box.
- Select the Reboot on Uninstall option if the patch that you are removing requires an immediate reboot. Keep in mind that other patches can be directly applied after this patch, so be sure to check this option if it is necessary.

7. Click Next to upload the patch. A progress bar appears.

8. After the patch is uploaded, you have the option to install the patch, as Figure 11-5 shows. Click Yes to install the patch, and then click Next. Otherwise, click No or click Close.

Figure 11-5: Upload Successful Message



Upload Successful

q251170_w2k_sp1_x86_en.exe has been successfully uploaded.

Would you like to install the patch next?

○ Yes ● No

Remember that if you need to upload the same patch for multiple versions of the same operating system, you must repeat this process with the same patch.

About Testing Patches

After you upload the patch, you can install and test it using the Patch Install Wizard. As the patch administrator, you can install the patch, even though the patch is automatically set in the Untested state after you upload it the first time. When you finish testing the patch, use the Opsware Command Center to change the patch state to available so that system administrators can install the patch.

Patch Administration Using the Opsware Command Center

This section provides information on patch administration within Opsware SAS and contains the following topics:

- Overview of Patch Administration
- Patch Statuses Overview
- Editing Patch Options Overview
- About Patch Installation Order Dependencies
- Creating Patch Installation Order Dependencies

Overview of Patch Administration

The Opsware Command Center allows you to search though all patches that have been uploaded. In addition, it lists patches from the Microsoft database that have not yet been uploaded. You can use the Opsware Command Center to edit patch options and create install order dependencies, and change the state of patches to *Available for Use* so that system administrators can install them. You can also view detailed information about individual patches, such as the number of times the patch has been installed.

Patch Statuses Overview

The patch administrator sets the status of a patch in Opsware SAS. The status determines who can apply the patch, or if the patch can be applied at all. (One additional state, *Not Yet Uploaded*, is set automatically and applies only to Windows patches).

Table 11-5 describes the statuses that patches in Opsware SAS can have.

Table 11-5: Patch Statuses in Opsware SAS

STATUS	DESCRIPTION
Untested	Initial state of a patch after being uploaded. Only administrators with special privileges can install untested patches.
Available for Use	Has been uploaded and approved by the patch administrator and can be installed on servers.
Not yet uploaded (Windows only)	A patch is described in the Microsoft Patch Database for one of the products that you have selected to track. This patch, however, has not yet been uploaded and cannot be installed. (This status is set automatically.)
Deprecated	The patch is possibly still installed on some systems, but cannot be installed anymore, not even by a user who is a member of the Advanced User role.

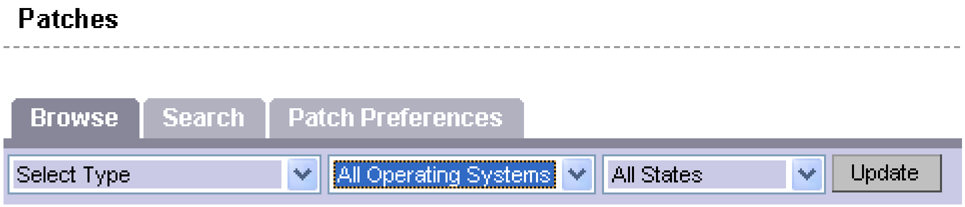
Setting Patch Status

Perform the following steps to set the patch status:

1. From the navigation panel of the Opsware Command Center, click Software ➤ Patches. The Patches page appears.

2 Select the filter options from the drop-down menus to display the type of patch whose status you want to change. You select the patch type, the operating system version, and the patch state. See Figure 11-6.

Figure 11-6: Search Example



Patches

Select Type | All Operating Systems | All States

3 Click Update to display the list of patches that meet your selection criteria.

4 Locate the patch and click the name of the patch. The View Patch page appears.

5 In the patch summary section of the View Patch page, click Edit. The Edit Patch page appears.

6 Select the desired status from the Patch Status drop-down menu and then click Save.

Editing Patch Options Overview

You can edit any of the options that you specified for a patch that you uploaded using the Patch Upload Wizard. Additionally, if you uploaded a patch with the OCLI, you can specify the same options for the patch by editing the patch options.

Some patch option are not editable, due to the nature of the patch type. For example, you cannot change the Reboot on Install option of a Windows Service Pack from yes to no, because it is set to yes automatically. You cannot set patch status on an HP-UX patch fileset because you can only set the patch status on the parent HP-UX patch product. (After you change the status of the parent HP-UX patch product, the change is applied to the children filesets.) Other options cannot be set because they do not apply to the patch type that you are editing.

Editing Patch Options

Perform the following steps to edit patch options:

1. From the navigation panel of the Opsware Command Center, click Software ➤ Patches. The Patches page appears.
2. Select the options from the drop-down menus to display the type of patch that you want to edit. You select the operating system version, the patch type, and the patch state.
3. Click Update to display a list of patches that match your selected criteria.
4. Locate the patch that you want to edit and click the link for the patch name. The View Patch page appears.
5. Click the Edit button to edit the patch options. (Click the Edit button in the Install Options or in the Uninstall Options, as appropriate.)
6. Add or modify the patch install or uninstall options and click save.

If you are modifying the options of a patch that you already marked as Available, consider resetting the status of the patch back to Untested. Test the patch again with the new options, and set the status back to Available when you determine that it is safe to install the patch again.

About Patch Installation Order Dependencies

For some patch types, install order dependencies can be set. You create installation order dependencies through the Opsware Command Center.

To add patch dependencies to a patch, you must first upload the patch using the Patch Upload Wizard. You must then edit the patch through the Patches page.

Creating Patch Installation Order Dependencies

Perform the following steps to create patch installation order dependencies:

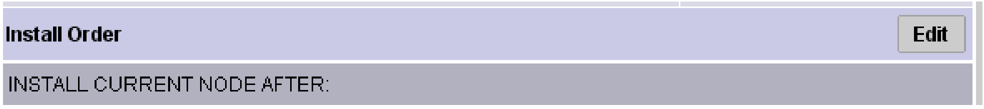
1. From the navigation panel of the Opsware Command Center, click Software ➤ Patches. The Patches page appears.
2. Select the options from the drop-down menus to display the type of patch that you want to edit. You select the operating system version, the patch type, and the patch state.

3. Click Update to display a list of patches that match your selected criteria.

4. Locate the patch that you want to edit and click the link for the patch name. The Patch Summary page appears.

5. Click the Edit button in the Install Order section. See Figure 11-7.

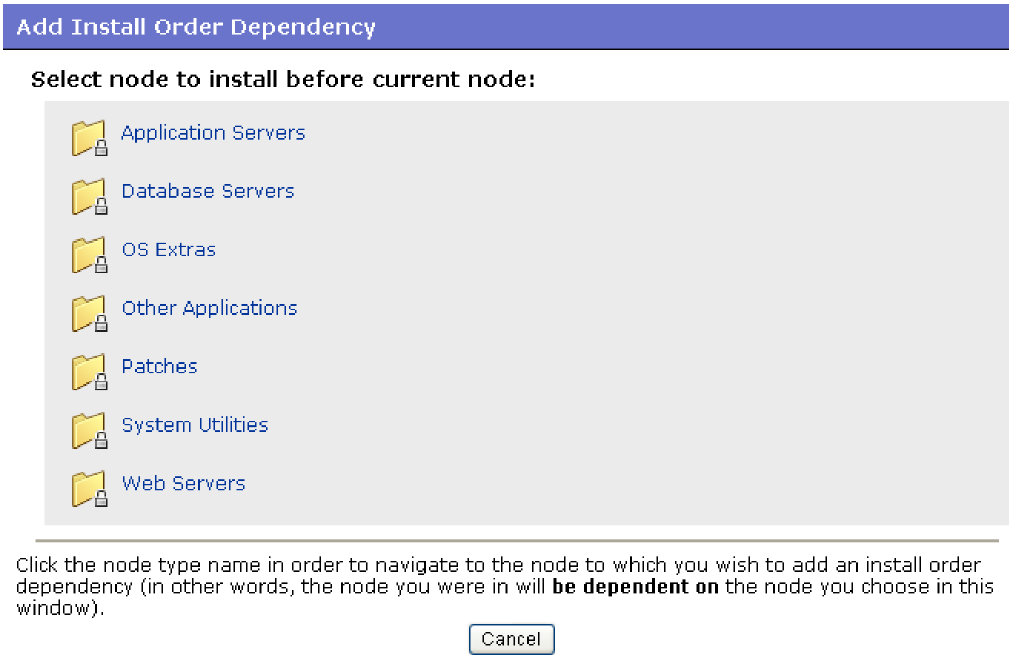
Figure 11-7: Install Order Section



INSTALL CURRENT NODE AFTER:

6. Click the Add button to select the type of software that must be installed before the selected path. See Figure 11-8.

Figure 11-8: Software Type



Add Install Order Dependency

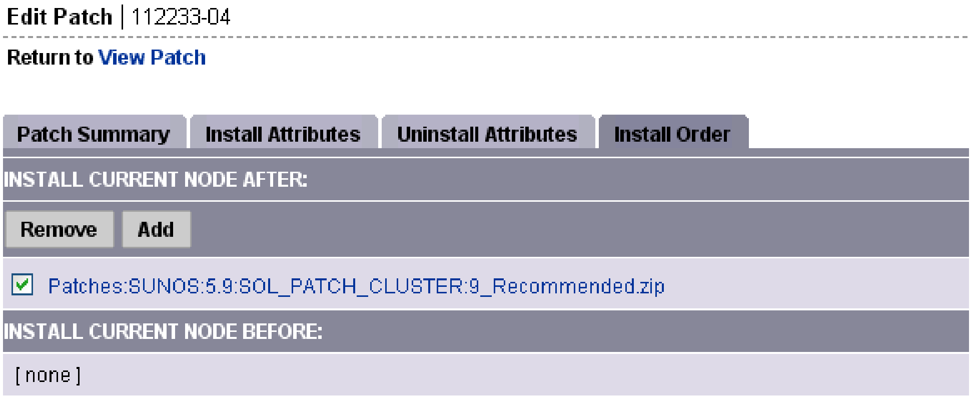
Select node to install before current node:

Click the node type name in order to navigate to the node to which you wish to add an install order dependency (in other words, the node you were in will **be dependent on** the node you choose in this window).

7. Browse for the software package or patch that must be installed before your selected patch.

8 Click the check box next to the desired software package and then click Add. See Figure 11-9.

Figure 11-9: Adding Install Order Dependency



☑ Patches:SUNOS:5.9:SOL_PATCH_CLUSTER:9_Recommended.zip

[none]

9 Confirm the dependency by clicking Add in the View Patch page. If you click Add again, the confirmation page does not appear. You will instead see the Add Install Order Dependency page, which allows you to add more packages.

10 Repeat the process if other dependencies must be expressed.

Chapter 12: Code Deployment Setup

IN THIS CHAPTER

This chapter discusses the following topics:

- Opsware Code Deployment Process
- Overview of Code Deployment & Rollback Setup

You must have specific permissions to setup code and content by using the Opsware Command Center. Contact your Opsware administrator to obtain the necessary access rights.

Opsware Code Deployment Process

This section provides information on the code deployment process within Opsware SAS and contains the following topics:

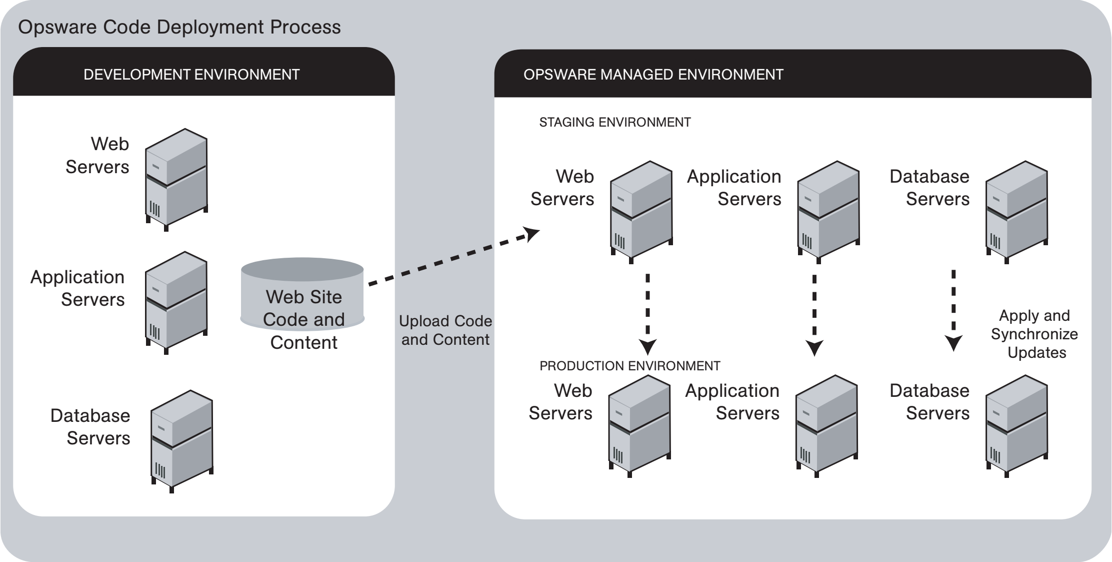
- Overview of Code Deployment Process
- Uploading Code and Content to Staging
- Using Code Deployment & Rollback
- Accessing Code Deployment & Rollback

Overview of Code Deployment Process

The Code Deployment & Rollback (CDR) feature in the Opsware Command Center provides tools for deploying new and updated code and content to your operational environment.

The following figure shows the architecture and process for updating a typical server hosted in an Opsware managed environment.

Figure 12-1: Typical Code and Content Update in the Opsware Managed Environment



The deployment process involves performing the following high-level tasks:

1. Determining your application code and content deployment requirements and defining the CDR services, synchronizations, and sequences that you need to support them

    - Services are defined for each different type of Web server or application server applications (for example, WebLogic Server) that is installed on the staging and production hosts in your environment.
    - Synchronizations are defined for each service so that you can update files between the source location and one or more destination production hosts that are running the same service.
    - Sequences are optional but can simplify deployment by grouping a collection of service operations and synchronizations that can be performed as a single task.

2. Uploading new or updated code and content to your Opsware staging environment

3. After performing any necessary testing, cutting over to the changed code and content on the staging environment

4. As necessary, performing CDR service operations, such as backing up code and content from your live site
5. Performing CDR operations available to synchronize the updated code and content to your production hosts in the Opsware managed environment
6. To simplify subsequent deployments of new code and content, defining sequences that specify a series of service operations and synchronizations you want to perform as a single action

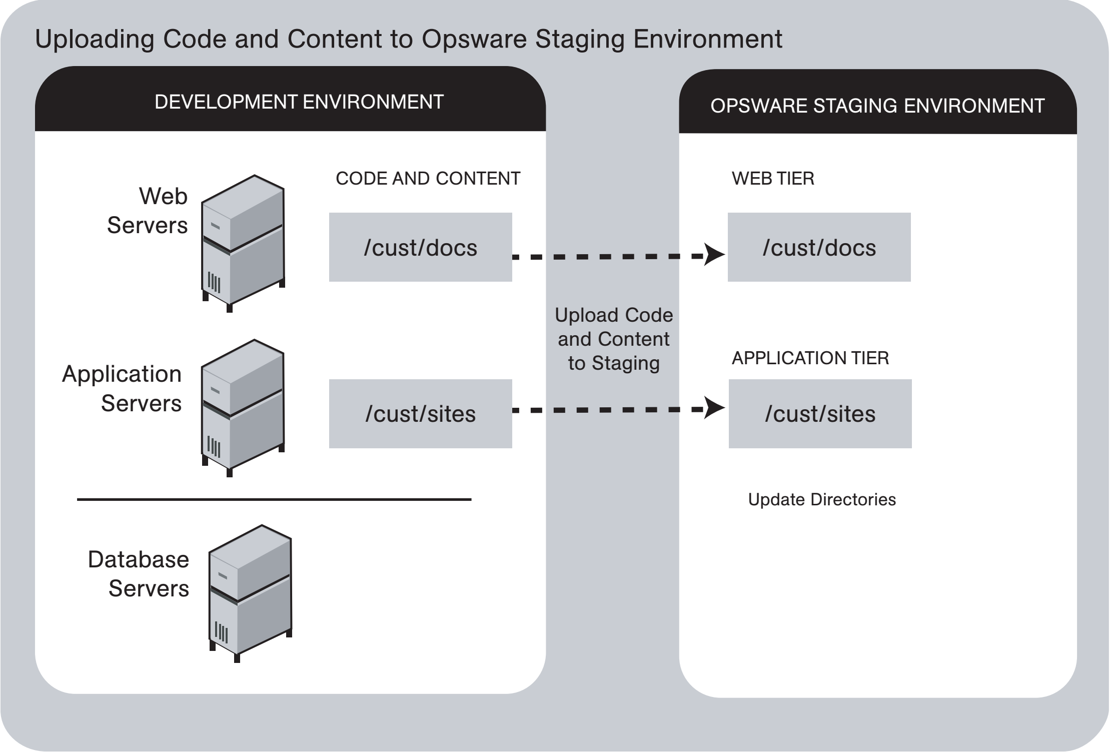
The code and content deployment process that you follow might be different depending on the architecture of your operational environment and your deployment requirements.

Uploading Code and Content to Staging

Before you use CDR to push code and content, you must upload new or updated files to your Opsware staging environment. You can use content management tools, such as OpenDeploy, scp, or rsync over SSH, to do that.

The following figure shows an example of a typical development environment and how your uploaded code and content move to the staging environment.

Figure 12-2: How Code and Content Move to the Staging Environment



After you upload the files and test your changes, you can synchronize updates to the production hosts running your managed environment. You can run specific synchronizations and perform other service deployment operations by selecting CDR menu options available from the Opsware Command Center navigation panel.

Using Code Deployment & Rollback

After you upload updated code and content to your Opsware-managed staging environment, you can use the CDR operations to cutover to new code and content, perform host synchronizations, and perform other service operations.

CDR uses the following directories to synchronize and cutover code and content for specified hosts:

- **Live directory** – The directory that stores the actual code and content required to run a live site.

- **Update directory** – The directory written to by CDR synchronizations. Stores only the files that changed between the source host Live directory and the Live directories of the destination hosts.
- **Site Previous directory** – This directory holds all the changes necessary to revert the Live directory back to the state it was in before the last cutover. Like the Update directory, the Site Previous directory only stores the files that changed between the current Live directory contents and its previous state.
- **Site Backup directory** – This directory stores a complete backup of the site. The directory is populated when the user issues a Backup service operation.

When you cutover to new code and content, CDR determines the differences between the new code and content in the current Update directory and the Live directory for your site. The files that are different are synchronized to the Live directory. When you synchronize source and destination hosts, CDR moves modified files from the Live directory on a source host to a directory on a destination host.

You cannot use CDR to automate database pushes. However, you can configure CDR so that you can synchronize modified database script files on different hosts.

CDR offers the following features:

- Provides a single tool for deploying code (such as ASP, JSP, and JAR files) and site content (such as HTML, JPEG, GIF, and PDF files). Using a single tool is helpful when the code and content for your site are intermingled.
- Provides direct control over code and content pushes by making it possible to decide what information to update and determine when and how to perform updates.
- Provides flexibility to accommodate frequent updates to staging and production hosts by enabling more frequent pushes in a shorter period of time.
- Allows verification of file changes between staging and production host directories by creating a manifest of updated files. You can verify changes before cutting over to new code and content.
- Provides administrative service operations, including starting and stopping services, and backing up, restoring, and rolling back code and content to return your site to the previous version.

- Lets you push incremental updates to your site so that only files that have changed are pushed to specified locations on staging or production hosts.
- CDR uses the same authentication and navigation that you use in accessing other information and performing other site operations from the Opsware Command Center.

Accessing Code Deployment & Rollback

As with all other features in Opsware SAS, the links that you see on the Opsware Command Center Home page and the links that you see in the navigation panel are based on the permissions that you have in combination with the customer you are associated with.

If you do not have permissions for CDR, you cannot see the Code Deployment links on the navigation panel, the link called Deploy Code in the Tasks panel of the Opsware Command Center home page appears in italics, and it is not an active link.

If you have CDR permissions to no more than one customer, when you expand the Code Deployment section in the navigation panel, you can see a link called Set Customer. Click that link to view the links to the specific Code Deployment functions that you have permissions for in combination with that single customer.

If you have CDR permissions to more than one customer, you can see a link called Select Customer. Click that link to display a page that shows the customers you are associated with. Select the customer you want to work with. The CDR Home Page appears, with links to the specific Code Deployment functions that you have permissions for. These links are the same functions that you can find in the navigation panel under Code Deployment.

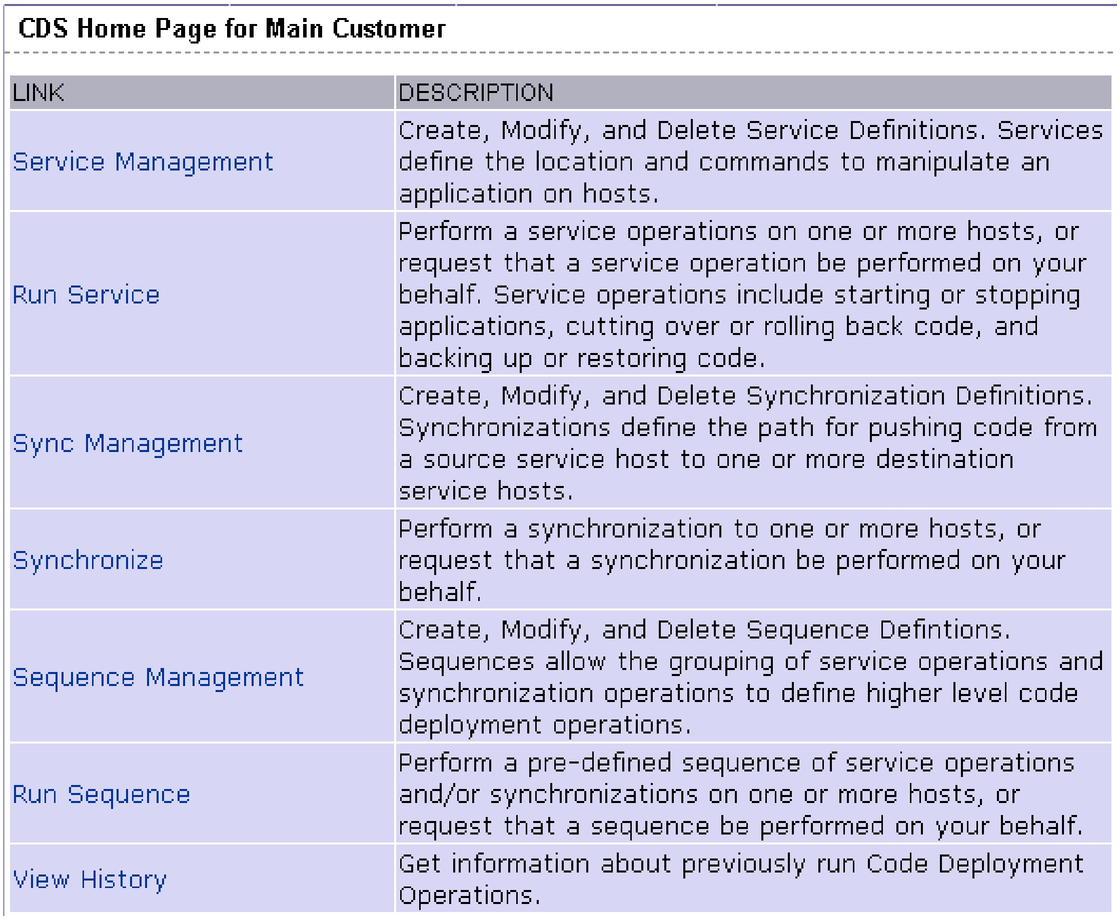
The navigation instructions and screen captures in this chapter show what a user with permissions to all code deployment functions and access to only one customer can see. Consequently, because your permissions and customers might be different, the available menu selections and features that you see might likewise differ.

Perform the following steps to access CDR:

1. If necessary, click the Code Deployment link in the navigation panel to expand the list of CDR options.

2 Click the CDR Home link. The CDR Home Page for [*customer name*] appears, as the following figure shows.

Figure 12-3: Code Deployment Home Page



CDS Home Page for Main Customer

LINK	DESCRIPTION
Service Management	Create, Modify, and Delete Service Definitions. Services define the location and commands to manipulate an application on hosts.
Run Service	Perform a service operations on one or more hosts, or request that a service operation be performed on your behalf. Service operations include starting or stopping applications, cutting over or rolling back code, and backing up or restoring code.
Sync Management	Create, Modify, and Delete Synchronization Definitions. Synchronizations define the path for pushing code from a source service host to one or more destination service hosts.
Synchronize	Perform a synchronization to one or more hosts, or request that a synchronization be performed on your behalf.
Sequence Management	Create, Modify, and Delete Sequence Defintions. Sequences allow the grouping of service operations and synchronization operations to define higher level code deployment operations.
Run Sequence	Perform a pre-defined sequence of service operations and/or synchronizations on one or more hosts, or request that a sequence be performed on your behalf.
View History	Get information about previously run Code Deployment Operations.

Depending on your access permissions, the following CDR options appear:

- Service Management – create, modify, or delete service definitions that define the location and commands to manipulate an application on hosts associated with each application instance running in your operational environment
- Run Service – perform a service operation or request that one be performed
- Sync Management – create, modify, or delete synchronization definitions associated with code pushes
- Synchronize – perform a synchronization or request that one be performed

- Sequence Management – create, modify, or delete sequences of operations
- Run Sequences – perform a selected sequence or request that one be performed
- View History – view information stored in an operations log to determine the status of particular deployment operations, and whether they completed successfully.

3 Choose the CDR operations that you want to perform, selecting options from the navigation panel or from the CDR home page.

Overview of Code Deployment & Rollback Setup

This section provides information on how to set up and support sites that use CDR for code and content pushes. It contains the following sections:

- Overview of Code Deployment & Rollback
- Code Deployment Configuration Checklist
- Deployment and CDR Configuration Procedures
- CDR Configuration Steps
- Determining Your Code and Content Deployment Requirements
- Planning Your CDR Configuration
- Preparing Host Machines
- Creating or Verifying Directories on Hosts
- Populating Initial Content in Directories
- Setting up Access Control for CDR
- Defining CDR Services, Synchronizations, and Sequences
- Defining and Modifying CDR Services
- Defining a Service
- Running Pre- and Post-Synchronization Scripts
- Modifying a Service
- Deleting a Service
- Creating and Modifying CDR Synchronizations
- Defining a Synchronization

- Modifying a Synchronization
- Deleting a Synchronization
- Creating and Modifying CDR Sequences
- Defining a Sequence
- Modifying a Sequence
- Deleting Sequences
- Verifying and Troubleshooting CDR Configuration

Overview of Code Deployment & Rollback

In configuring CDR for a specific site, you first need to install and configure required software on each of the host machines used in your Opsware managed staging and production environment. Then, you define the set of services, service operations, and staging and production server synchronizations and sequences to make available.

By selecting Service, Synchronization, and Sequence options from the CDR menus, users can either perform operations or request that other authorized users perform them. (Permissions to perform specific CDR operations depend on the code deployment user groups to which individual users are assigned.)

See “Code Deployment Permissions” on page 60 in Chapter 3 for information about how to create users and assign the Opsware Command Center permissions.

The instructions provided in this chapter are intended to be platform-neutral. However, platform-specific information and examples are provided where necessary.

The preparation of host machines, directory configuration, and testing should all be carried out during scheduled maintenance windows because modifications made to production machines might cause downtime for the live site.

Code Deployment Configuration Checklist

Before you set up your site to use CDR, collect the following information about the site:

- Names of all host machines used for a site and their designation for use as staging, QA, production, and so forth
- All service instances installed for a site (for example, WebLogic, iPlanet Web Server, and so forth)
- All top-level code and content directories that are used by each of the service instances. (Directories are based on the service or service instance and are the same on all host machines where a particular service or service instance is installed.)
- The name of the machine and directory location where site code and content is uploaded. (This is the host and directory location where you upload files from your own development environment, using an Opsware-supported content deployment tool such as OpenDeploy, scp, or rsync over SSH.)

Make sure that you have identified an appropriate process to upload changed code and content from your development environment and check that the appropriate firewall conduits and connections are created to allow uploading changed code and content into the site.

- For a new site deployed in an Opsware managed environment, you should also obtain a copy of your site's current code and content to preload into directories prior to using CDR. Preloading code and content shortens the time required to complete updates the first time that you use CDR to perform synchronizations.

Deployment and CDR Configuration Procedures

The overall process for planning and defining a CDR configuration and using CDR to define services and synchronizations for your site consists of the following tasks:

1. Determine your site's code and content deployment requirements.
2. Define the services and synchronizations that are needed to support your site requirements. Optionally, define any sequences of both services and synchronizations that you would like users to define as sequences so users can perform them in a single step.
3. Upload new or updated code and content to the Opsware staging environment.

4. Cutover to the changed code and content on the staging environment and perform any required testing.

5. As necessary, you can also set up email notification to send requests to select users to perform CDR service operations, such as backing up code and content from their live site and synchronizing the updated code and content to their production hosts.

Your Opsware administrator determines the responsibilities that different users have pertaining to synchronizations and other service operations performed for a specific site.

CDR Configuration Steps

The following summary shows the steps involved in configuring a site to use CDR for code and content updates, code pushes, and other service/synchronization operations.

The sections that follow described each of the steps in detail:

1. Determine your code and content deployment requirements.

   Determine the responsibilities that users who are assigned to perform synchronizations, sequences, and other service operations will have.

2. Plan your CDR configuration.

   Create diagrams of your site's host configuration, specifying synchronization and service descriptions, including any special service operations that you want carried out when a specific synchronization or sequence is performed.

   See "Planning Your CDR Configuration" on page 361 in this chapter for information about how to document your CDR configuration and the services, synchronizations, and sequences you are creating for your site.

3. Set up access control for CDR.

   Have your Opsware administrator create and add users to user groups to create, edit, request, or perform CDR services, synchronizations, and sequences. (User groups that have specific permissions to perform CDR operations are predefined.)

4. Create Services and Synchronizations in CDR.

   Using the service, synchronization, and sequence documentation defined for your site, create each service, synchronization, and sequence in CDR. Assign the user groups required to access each service, synchronization, or sequence when a user logs into the Opsware Command Center.

See “Defining CDR Services, Synchronizations, and Sequences” on page 369 in this chapter for more information.

5 Verify that the following port is accessible between the server you will push code from and the server where you will push code to:

- `telnet <staging_server> 1002`
- `telnet <production_server> 1002`

6 Configure email notification addresses.

Specify the email addresses where notifications are sent when users request that a service operation, synchronization, or sequence be performed on their behalf.

7 Test CDR setup and configuration.

After all services, synchronizations, and sequences are defined, and user accounts and permissions are set up in the Opsware Command Center, test the operations available for each service, synchronization, and sequence defined in CDR. Uploading both code and content changes from your site development environment, verify that CDR can be used to update services on all staging and production hosts for which synchronizations are defined.

Determining Your Code and Content Deployment Requirements

Discover your exact deployment requirements, and determine the responsibilities that users who are assigned to performing synchronizations and other service operations will have.

Depending on the setup of your site, you might want certain users to perform routine content updates to your site and assign responsibility for more critical application code changes to other users who will, for example:

- Perform service operations for your production site
- Synchronize updated code and content to your production site
- Run sequences that perform a sequence of service operations and sequences as a single step

CDR lets you send email requests to specific users, notifying them to perform a synchronization, sequence, or other service operation.

The options that are available to users when they access CDR depend on the user groups and permissions the users have been assigned.

See “Code Deployment Permissions” on page 60 in Chapter 3 for information about how to create users and assign Opsware Command Center permissions.

Planning Your CDR Configuration

Before you can use CDR, define the services and synchronizations you need to update and maintain your site. You define individual services based on each specific Web server or application server application (for example, WebLogic Server) that is installed on the staging and production hosts. You define synchronizations so that you can update files for a given service between the source location and one or more destination production hosts.

To define CDR services and synchronizations, you need to know:

- What the code and content directories are for each host
- Which hosts for your site are staging, production, and QA
- What services (for example, Web server or application server programs) are installed on each server

When you login to the Opsware Command Center, CDR displays predefined services and synchronization that are available for your site. You see only the services and synchronization that you have authorization to perform because of your user group membership.

The operations that you need to perform are specific to the service (Web server or application server instance) for which you are updating code or content and to the particular host.

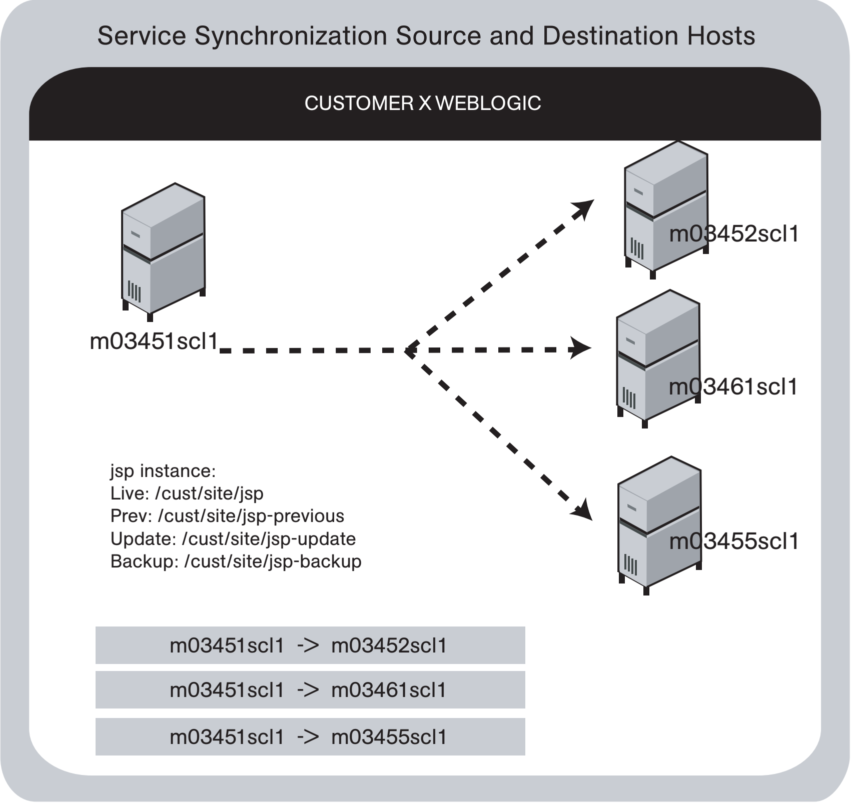
Before you use CDR to define services and synchronizations, you should document and diagram your site’s configuration. That way, when you start defining services and synchronizations, the process is likely to go more smoothly.

To plan your CDR configuration, complete the following tasks for every instance of a service (for example, WebLogic application server or iPlanet Web server):

1. Create a diagram of your site’s host configuration for the service, designating the source and destination hostnames for any synchronizations that you want to define.

Figure 12-4 shows an example of a typical synchronization diagram defined for a specific service, in this case, a WebLogic (jsp) application instance.

Figure 12-4: Service Synchronization Source and Destination Hosts



In the diagram, all three arrows are part of the same synchronization and specify update paths from the source to the destination host. The diagram also specifies the site's Live, Previous, Update, and Backup directories used by the instance in performing synchronizations, backup, restore, and rollback operations.

2 List the service directories, scripts, and any special operations or procedures to be performed for any synchronization of code or content for that service.

Table 12-1 shows the information that you can specify for a service defined in CDR.

Table 12-1: Table of Information to Specify for Code Deployment Service

SECTION OF PAGE	FIELD NAME
Service	
	Name (required)
	Type (required)
Service Commands	
	Start
	Stop
	Pre-cutover
	Post-cutover
	Pre-rollback
	Post-rollback
	Pre-Sync To Update
	Post-Sync To Update
	Pre-Sync To Live
	Post-Sync To Live
	Pre-backup
	Post-backup
	Pre-restore
	Post-restore
Service Directories	
	Live Directory (required)
	Update Directory (required)
	Backup Directory (required)
	Previous Directory (required)

Table 12-1: Table of Information to Specify for Code Deployment Service

SECTION OF PAGE	FIELD NAME
Service Hosts	
	Hosts
Roles	
	Perform Role Name (required)
	Request Role Name (required)
Service Options	
	CC Operation Requests To

3 Determine the name that you want to give the synchronization when you create it by using CDR, for example, WebLogic Sync (Staging to Production). You should designate the user groups whose members can request or perform the synchronization.

Table 12-2 shows information that you can specify for synchronizations defined in CDR.

Table 12-2: Table of Information to Specify for Synchronizations

SECTION OF PAGE	FIELD NAME
	Name (required)
	Associated Service Name
	Source Host Type (required)
	Source Host (required)
	Destination Host(s) Type (required)
	Destination Host(s) (required)
	Perform Role Name (required)
	Request Role Name (required)
Options	
	CC Operation Requests To
	Strict Synchronization

4 Repeat the process to create additional diagrams for each instance available in your site environment for which you want to be able to push code or content.

Documenting your plans for code and content deployment for your site will simplify the process of defining new services and synchronizations when you access CDR. Distributing this information to other users provides useful documentation of your site's configuration, so that everyone involved in code and content deployment for your site understands what services are defined and what synchronizations are available to push code and content.

Preparing Host Machines

After you determine the CDR configuration of services and host machines for your site, perform the following tasks:

- Prepare each host machine in that configuration so that CDR can perform the synchronizations and service operations that you define.
- Create or verify the existence of Live, Previous, Update, and Backup directories on all source and destination hosts.

Creating or Verifying Directories on Hosts

Before you perform synchronization, you must create or verify that the Live Directory, Previous Directory, Update Directory, and Backup Directory already exist on all source and destination hosts. Using the list of host machine names that you collected for your site, login to each of the hosts and check that all the directories already exist or create them.

To determine disk space requirements for a site, you can estimate that CDR requires between two and four times the total size of code and content installed on a particular host, depending on CDR usage factors such as number of changed files between synchronizations and cutovers, use of backup features, and so forth.

- The Live Directory is the directory used for deployed code and content on your site (for example, `/cust/docs` for a Web server, `/cust/site` for an application server like WebLogic).

- The Previous Directory is the directory that records the difference between the current Live Directory's code and content and the version of the site as it existed prior to the last cutover.
- The Update Directory is the directory written to by a CDR synchronization that records the difference between the Live Directories on the source and destination systems.
- The Backup Directory is the directory used to store files when users request a backup copy of the current code and content Live directory.

Ownership of the Live, Previous, Update, and Backup directories is not important because CDR software used to perform service operations and synchronizations runs as root.

Populating Initial Content in Directories

After you create directories on all the hosts designated for a new site deployment (staging, QA, production hosts), you should populate the Live directories on each host with the initial code and content for the site.

Archive a copy of the site files and use a file transfer utility to perform the initial site upload. Using CDR synchronization to initially populate directories has significant overhead and might take longer to perform than directly copying the initial site code and content.

This step (populating directories) only applies to setting up new sites, because current code and content for your site is already available on the Opsware staging and production hosts.

In a Unix environment, you can tar the files and use scp to perform the initial site upload into each host Live directory. In a Windows environment, use the Windows file transfer utility to do the initial site upload when you configure host machines for a new deployment.

Setting up Access Control for CDR

CDR uses the Opsware Command Center authentication to control users' access and ability to perform service operations and synchronizations. Specific permissions to perform code deployment operations are based on a user's membership in predefined

CDR user groups, which an Opsware administrator defines in the Administration section of the navigation panel. Table 12-3, Table 12-4, Table 12-5, and Table 12-6 provide descriptions of permissions that are associated with predefined CDR user groups.

Table 12-3: Special Code Deployment User Groups

CDR USER GROUP	DESCRIPTION
Super-User	Users in this user group can define, request, or perform any code deployment operation on hosts for any customer.
History Viewer	Users in this user group can view a log of operations (service operations, synchronizations, and sequences) that were executed from the Code Deployment feature. Viewing this information can help you determine the completion status of particular deployment operations.

Table 12-4: Service User Groups

CDR USER GROUP	DESCRIPTION
Service Editor	Users can define services and modify or delete service definitions.
Service Performer (Production)	These users directly perform or request performance of service operations on hosts designated for use in production.
Service Performer (Staging)	These users directly perform or request performance of service operations on hosts designated for use in staging.
Service Requester (Production)	These users directly request performance of service operations on hosts designated for use in production.
Service Requester (Staging)	These users request performance of service operations on hosts designated for use in staging.

Table 12-5: Synchronization User Groups

CDR USER GROUP	DESCRIPTION
Synchronization Editor	Users can define a synchronization, modify, or delete the synchronization definition.
Synchronization Performer	These users directly perform or request performance of synchronization actions.
Synchronization Requester	These users request performance of synchronization actions.

Table 12-6: Sequence User Groups

CDR USER GROUP	DESCRIPTION
Sequence Editor	Users can define sequences, and modify or delete sequence definitions.
Sequence Performer (Production)	These users directly perform or request performance of sequences of actions on hosts designated for use in production.
Sequence Performer (Staging)	These users directly perform or request performance of sequences of actions on hosts designated for use in staging.
Sequence Requester (Production)	These users request performance of sequences of actions on hosts designated for use in production.
Sequence Requester (Staging)	These users request performance of sequences of actions on hosts designated for use in staging.

When a user submits CDR requests asking that a service operation or synchronization be performed on the user’s behalf, an email notification is sent to the individuals assigned to perform the requested service operation or synchronization. See “Code Deployment Permissions” on page 60 in Chapter 3 for information about how to assign users to predefined CDR user groups.

Each user group is created without any users initially added. Your Opsware administrator can add individual users to each CDR user group to control their permissions to request or perform service operations, synchronizations, and sequences.

See “Code Deployment Permissions” on page 60 in Chapter 3 for information about how to add users to CDR user groups.

When a user selects a CDR option, Opsware SAS determines the user's user group memberships and determines what service and synchronization actions the user can perform. Depending on user group membership, the user can either (1) perform or request performance of a service management operation or synchronization operation, or (2) request that the operation be performed by users specified in an email notification list.

Defining CDR Services, Synchronizations, and Sequences

By using the list of services and synchronizations that you have planned for your site, you can use CDR to create the corresponding service and synchronization definitions in the Opsware Command Center.

You should follow this process:

1. Create all the services required for your site. Each service is defined in terms of the commands such as start or stop that are required for the associated service instance.
2. After you define all services, create all synchronizations that you want to make available. Each synchronization references a specific service and specifies the source host from which the service’s directories and files are to be synchronized to one or more destination hosts.
3. After you define services and synchronizations, define sequences to specify a sequence of specific service and synchronization operations that you want to perform as a unit.

See “Planning Your CDR Configuration” on page 361 in this chapter for information about how to define the services and synchronizes that you need to create for a particular site.

Defining and Modifying CDR Services

The CDR Service Management option lets you create new services or modify or delete existing services. For example, if you have a single instance of a service, you can use CDR to define a single CDR service. If you have five instances of a service, you can define five individual CDR services.

You should also create different services to provide control over services performed on staging hosts versus production hosts. For example, you could define a service that only names staging hosts and specify a *perform* user group for users who can perform operations for those hosts. You could then define a second service that names all hosts (both staging and production) and limit the perform user group to selected users.

In CDR, every service is defined down to the level of a single command that needs to run during service operations, such as start, stop, pre-cutover, post-cutover, and so forth. Both services and service instances are defined the same way because conceptually there is no difference between them. For example, you can define an Apache service, or several instances of ATG Dynamo or BEA WebLogic in terms of the scripts required to start or stop the service and scripts to perform at pre-cutover, post-cutover, and so forth.

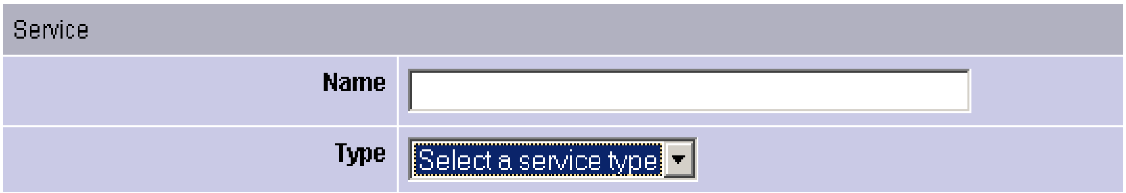
Defining a Service

If you are invoking Python in a CDR service command, you must invoke Python by using a fully qualified path to `python.exe` in the command. If you are migrating to the current version of Opsware SAS from a previous version, you must update any currently defined CDR service commands.

Perform the following steps to define a service:

1. Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
2. Click the Service Management option.
3. Click the Define a New Service link. The CDR Service Name and Type page appears, as Figure 12-5 shows.

Figure 12-5: CDR Service Name and Type



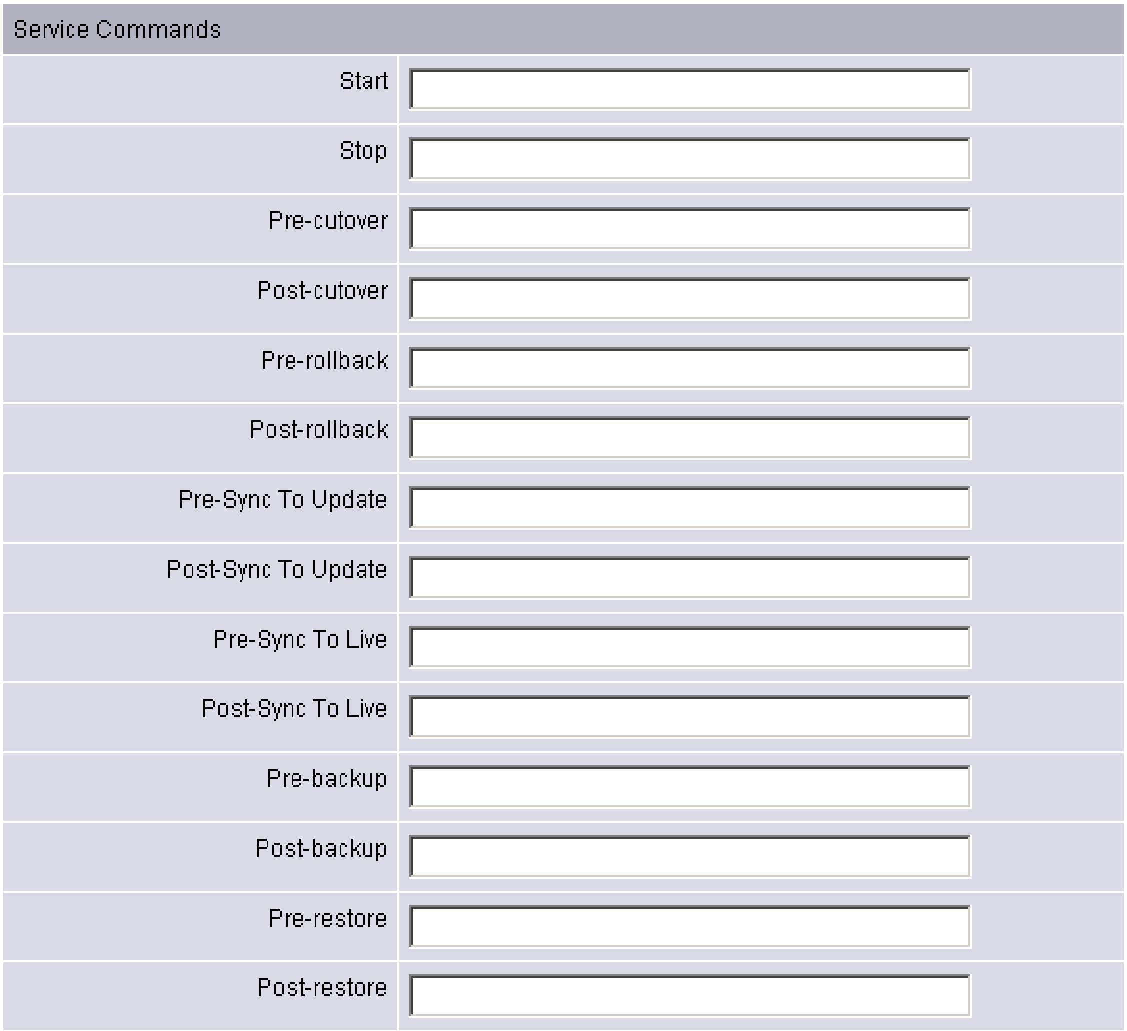
Service

Name	
Type	Select a service type

4. Specify the name of the service by choosing a name that users can identify with the corresponding application instance, for example, WebLogic (EJB Instance).

5 Specify the type of service that you want to create by selecting the service type from the drop-down list, as Figure 12-6 shows. The drop-down list includes the names of all application instances defined in the Model Repository.

Figure 12-6: CDR Service Commands



Service Commands

Start

Stop

Pre-cutover

Post-cutover

Pre-rollback

Post-rollback

Pre-Sync To Update

Post-Sync To Update

Pre-Sync To Live

Post-Sync To Live

Pre-backup

Post-backup

Pre-restore

Post-restore

6 In the Service Commands section, enter any commands to perform for the specific service or service instance. In each case, you can enter a single command (specifying a fully qualified path) that is run to effect the operation. The same commands and scripts are applied for all hosts where the service is installed.

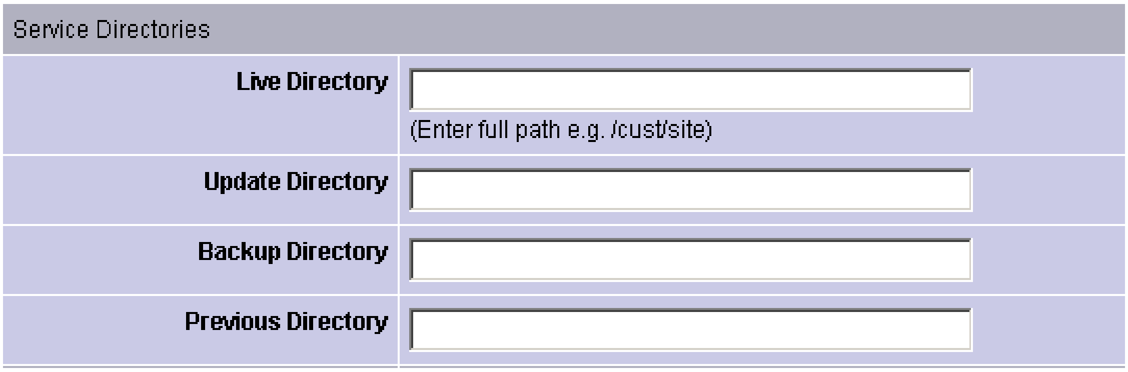
- Start and Stop fields – specify single commands or scripts that are executed when users choose the Service Management option to start and stop a specified service.
- Pre-cutover and Post-cutover fields – specify single commands or scripts that are executed before and after a user chooses the Run Service option to cutover code and content changes to Live.
- Pre-Rollback and Post-Rollback fields – specify single commands or scripts that are executed before and after a user chooses the Service Management option to restore code and content in a service's Live directory from the service's Rollback directory on specified hosts.
- Pre-Sync to Update and Post-Sync to Update fields – specify single commands or scripts that are executed before and after a user chooses the Synchronize option to synchronize code and content changes to the Update directory on specified hosts.
- Pre-Sync to Live and Post-Sync to Live fields – specify single commands or scripts that are executed before and after a user chooses the Synchronize option to synchronize code and content changes to the Live directory on specified hosts.
- Pre-Backup and Post-Backup fields – specify single commands or scripts that are executed before and after a user chooses the Service Management option to back up code and content from a service's Live directory to a Backup directory on specified hosts.
- Pre-Restore and Post-Restore fields – specify single commands or scripts that are executed before and after a user chooses the Service Management option to restore code and content from a service's Backup directory to the Live directory on specified hosts.

7 In the Service Directories section (see Figure 12-7), specify the disk locations for Live, Update, Previous, and Backup directories used by the service (common for all hosts where a given service is installed).

- Live Directory – the directory that stores the actual code or content required by a specific service to run a live site.
- Update Directory – the directory written to by CDR synchronizations. Stores files that changed between the source host Live directory and the Live directories on destination hosts where the service is installed.

- Backup Directory – the directory written to by CDR backup operations; used by the Restore option to return a service's Live directories to the code and content of a previous backed up version.
- Previous Directory – the directory written to by CDR cutover operations; used by the Rollback option to return a service's Live directories to the code and content that existed prior to the last performed synchronization.

Figure 12-7: CDR Service Directories



Service Directories

Live Directory

(Enter full path e.g. /cust/site)

Update Directory

Backup Directory

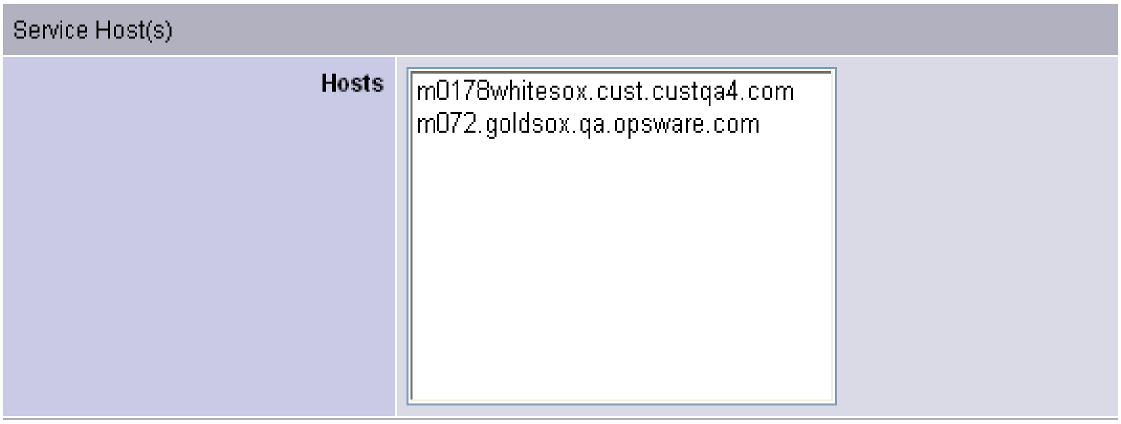
Previous Directory

8. In the Service Hosts section, select all hosts on which this service is running. You can use the Shift and Control keys to select multiple hosts. See Figure 12-8.

   These servers have a use field that has Code Deployment selected in Server Attributes.

   The servers also have a state of OK. If you changed the use of a server by using the Opsware Command Center, click the Refresh button to update the host list.

Figure 12-8: CDR Service Hosts



Service Host(s)

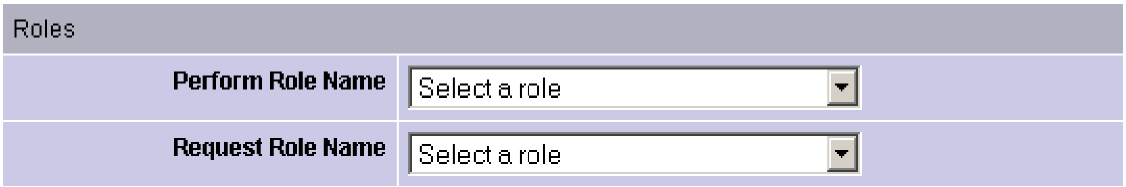
Hosts

m0178whitesox.cust.custqa4.com
m072.goldsox.qa.opsware.com

9 In the Roles section, specify the CDR user groups whose members you want to perform or request operations for the specific service. The Perform Role name determines the user group whose members can perform or request that select staff, or your Operations Center, perform a specific operation associated with the service. The Request Role Name specifies user groups whose members can request only an operation, such as start or stop for a service. See Figure 12-9.

See "Setting up Access Control for CDR" on page 366 in this chapter for information about the description of CDR user groups that you can specify for the Perform Role and Request Role names.

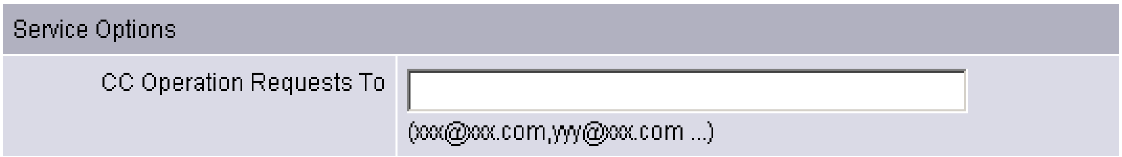
Figure 12-9: CDR Roles for Performers and Requesters



Roles

Perform Role Name	Select a role
Request Role Name	Select a role

Figure 12-10: Email Addresses to Copy CDR Operation Requests to



Service Options

CC Operation Requests To	(xxx@xxx.com,yyy@xxx.com ...)

10 In the Service Options section (see Figure 12-10), specify any email address contacts that you want to notify for any service operation requests.

Specifying email notifications allows flexibility in assigning requests to select members of your staff or your Operations Center.

11 When you finish making entries to define a new service, click the Save button.

CDR verifies that the service name you specified is unique and then saves the new service definition data in the Model Repository.

To save defined services, you must select at least one hostname and provide entries for the Service Name, Service Type, Start Service, Stop Service, Perform Role, and Request Role fields.

Running Pre- and Post-Synchronization Scripts

Pre- and post-synchronization scripts only run on destination hosts.

On Windows machines, you can use the post-cutover command, for example, to specify a command that performs Windows object registration (among other tasks). In that case, you might define a post-cutover script that (1) lists all files in a directory and (2) passes all files with the .dll extension to `regsvr32.exe` and passes all files with the .msi extension to `msiexec.exe`. Performing these steps registers and un-registers COM objects. A similar script can be developed to de-register and register COM+ objects. This script can be named in CDR and must then be placed on all hosts on which the service could run.

You can specify the instance name as a command line argument in Start and Stop commands or scripts for services that describe instances of the same service running on the same hosts. (You need to create different services for each service instance running on the same hosts because the directories and start and stop script calls used by each instance are different.)

Start and Stop and other service command or script entries: If you need to perform operations that require more than a single command, you should define a sequence of commands in a single script file and then specify that script in the CDR service definition.

Modifying a Service

Occasionally, you need to modify an existing service, for example, to change assigned hosts, make updates to scripts, or make other changes to the attributes of the service.

Perform the following steps to modify a service:

1. Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.

2. Click the Service Management option.

3. Click the Modify an Existing Service link.

4. Click the name of the service that you want to modify.

5. Update the field entries that you want to modify, and then click OK. A confirmation page appears.

   You can modify all field entries that define a service except for the Service Type field. If you modify the Service Name field to rename a service, CDR confirms that the new name is not already in use.

CDR deletes synchronizations associated with a service when the following modifications are made:

- When a user removes a hostname from the list of hosts defined for a service and that hostname is a source for a synchronization, that synchronization is also removed when the service definition is saved. If that synchronization is used by a sequence, then that sequence is also removed.
- When a user removes a hostname from the list of hosts defined for a service, and that hostname is the last remaining destination for a synchronization, that synchronization is also deleted when the service definition is saved. If that synchronization is used by a sequence, then that sequence is also removed.
- When a user removes a hostname from the list of hosts defined for a service, and that hostname is the last host in a sequence step, then the whole sequence is deleted when the service definition is saved.

Deleting a Service

CDR allows you to delete services and remove their stored definition from the Model Repository.

Perform the following steps to delete a service:

1. If necessary, click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
2. Click the Service Management option.
3. Click the Delete a Service option.
4. Select the check boxes next to the services that you want to delete and click Delete.

   CDR prompts you to confirm the deletion.
5. Click OK. CDR removes the services that you chose to delete.

If you request deleting a service definition, CDR displays a confirmation box that indicates that any associated synchronizations or sequences are also deleted when it deletes the service.

Creating and Modifying CDR Synchronizations

The CDR Sync Management option lets you create, modify, or delete synchronizations so that you can update files for a given service between a source host location and one or more destination hosts. For example, in setting up a synchronization for a WebLogic application server instance, you can create a synchronization to transfer updated files between a staging host and the production host machines used to run your site.

When defining a synchronization, you first select the service, then specify the source and destination hosts you want to synchronize. In addition, you specify the CDR user groups that can perform or request the synchronization. You can also specify options such as addresses for email notification of synchronization requests and how synchronizations are performed (Strict Synchronization transfers updated files and removes deleted files from destination hosts.)

Defining a Synchronization

Perform the following steps to define a synchronization:

1. Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.

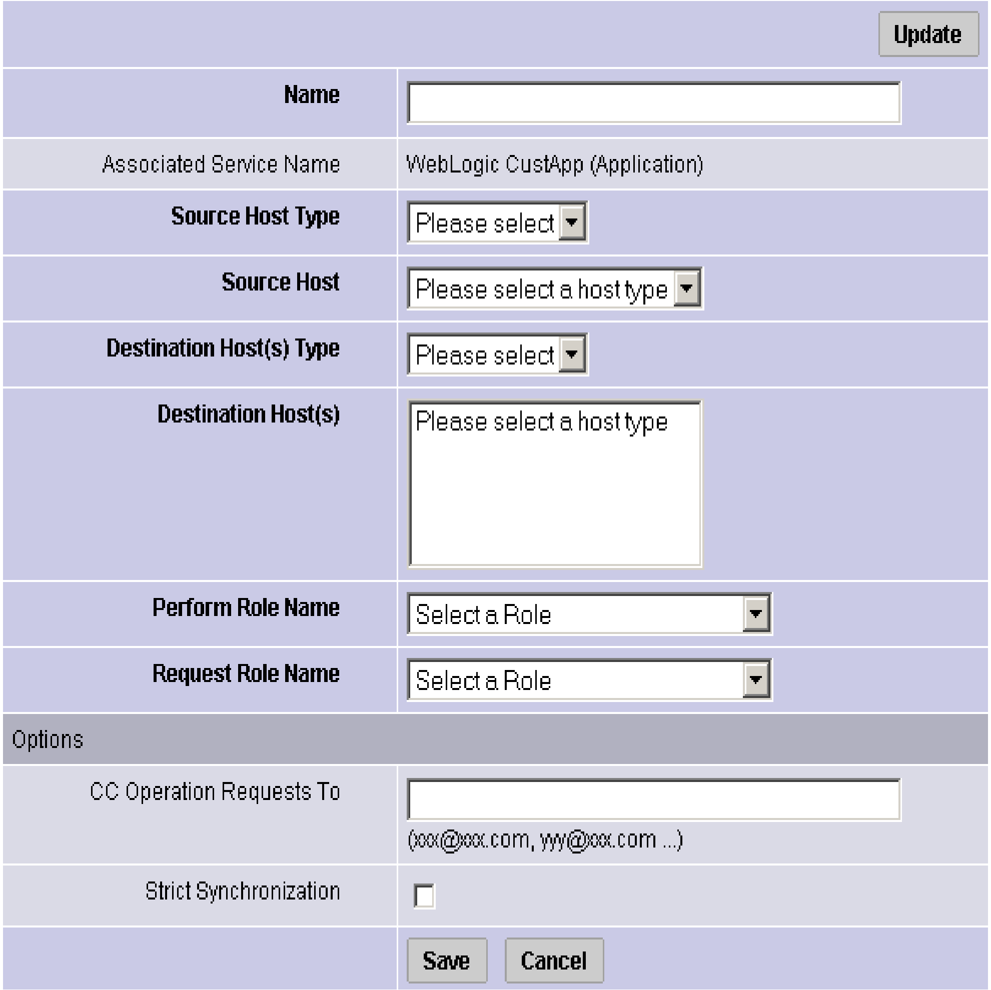
2. Click the Sync Management option.

3. Click the Define a New Synchronization option.

4. Select the service to which you want to add a synchronization.

   CDR displays a page on which you can define a new synchronization, choose source and destination hosts, and specify other synchronization options. See Figure 12-11.

Figure 12-11: Define a New Synchronization Page



	Update
Name	
Associated Service Name	WebLogic CustApp (Application)
Source Host Type	Please select ▾
Source Host	Please select a host type ▾
Destination Host(s) Type	Please select ▾
Destination Host(s)	Please select a host type
Perform Role Name	Select a Role ▾
Request Role Name	Select a Role ▾
Options	
CC Operation Requests To	(xxx@xxx.com, yyy@xxx.com ...)
Strict Synchronization	□
	Save Cancel

5 Specify the name of the synchronization, choosing a name by which users can identify the type of synchronization being performed, for example, WebLogic Sync (Staging to Production).

6 Specify the Source and Destination Host Types, choosing the type from the drop-down lists, which display all values stored in the Model Repository. These values are editable using Server Attributes.

You need to specify a Host Type before any hosts are displayed in the Source or Destination Host lists.

7. Specify the single Source Host for the synchronization from the list of hosts stored in the Model Repository that match the value that the Source Host Type specified.
8. Specify one or more Destination Hosts for the synchronization from the list of hosts stored in the Model Repository that match the value that the Destination Host Type specified.

Use the Shift and Control keys to select multiple destination host machines.

9. In the Perform Role Name and Request Role Name fields, select the CDR user groups that you want to allow to perform or request operations for the synchronization. The Perform Role Name determines the user group whose members can perform, or request that another member perform a particular synchronization. The Request Role Name specifies user groups whose members can request that authorized individuals perform synchronizations.

   See “Setting up Access Control for CDR” on page 366 in this chapter for information about a description of CDR user groups that you can specify for the Perform Role and Request Role Names.
10. In the Synchronization Options section, specify any email address contacts that you want notified of any synchronization requests.
11. Click the Strict Synchronization check box to specify that files deleted from the source host are also removed from corresponding directories on destination hosts defined in the synchronization. (Otherwise, if unchecked, the synchronization affects only files that are new or have changed between the source host and destination hosts and files removed from a source host are not removed from destination hosts.)
12. When you finish making entries to define a new synchronization, click the Save button. CDR verifies that the synchronization name that you specified is unique and then saves the new synchronization definition data in the Model Repository.

To save a new synchronization, you must specify a unique synchronization name, the source host and at least one destination host, and user groups that can perform or request synchronizations.

Modifying a Synchronization

Occasionally, you need to modify an existing synchronization, for example, to change source or destination hosts or make other changes to attributes of the synchronization.

Perform the following steps to modify a synchronization:

1. Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
2. Click the Sync Management option.
3. Click the Modify an Existing Synchronization option.
4. Click the name of the synchronization you want to modify.
5. Update the field entries that you want to modify, then click OK. A confirmation page appears.

When you modify a synchronization by removing a host from the list of destination hosts, and that host is the last host in a synchronization sequence step, then that sequence is removed.

You can modify all field entries that define a synchronization except for the Source and Destination Host Type fields. If you modify the Synchronization Name field to rename a synchronization, CDR confirms that the new name is not already in use.

Deleting a Synchronization

CDR allows you to delete synchronizations and remove their definition from the Model Repository.

Perform the following steps to delete a synchronization:

1. Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
2. Click the Sync Management option.
3. Click the Delete a Synchronization option.

4 Select the check boxes next to the synchronization that you want to delete and click Delete.

CDR prompts you to confirm the deletion.

5 Click OK. CDR removes the synchronizations that you chose to delete.

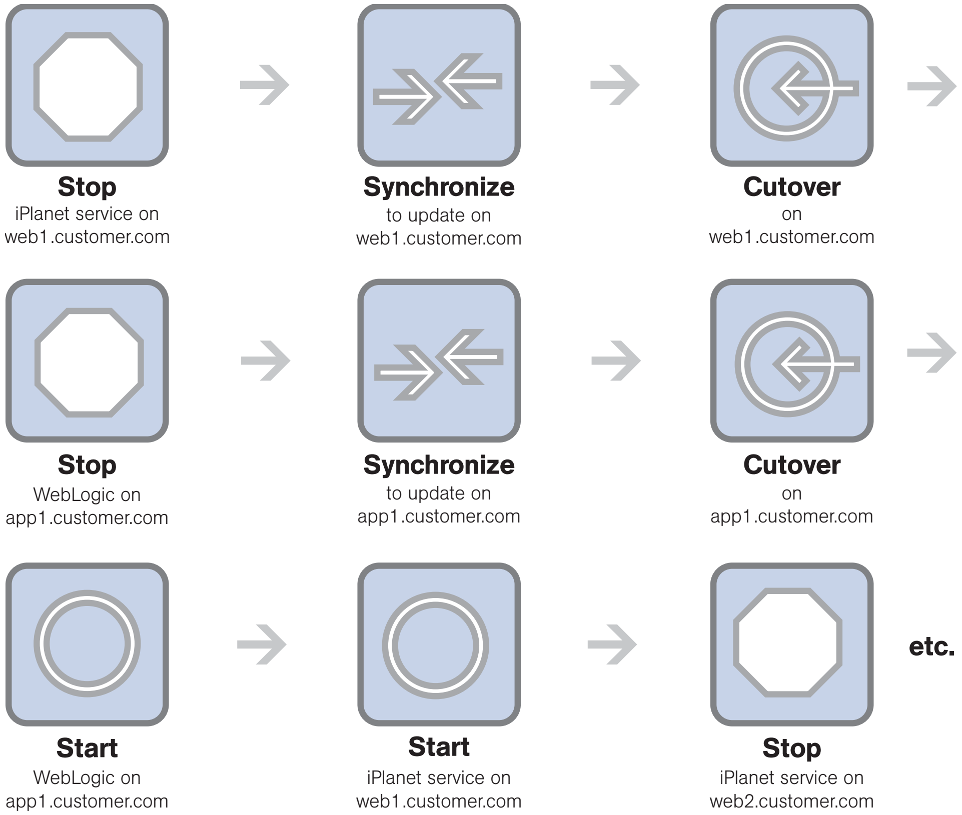
Deleting synchronizations that are used by a sequence causes that sequence to be deleted.

Creating and Modifying CDR Sequences

The CDR Sequence Management option lets you create, modify, or delete sequences of service operations and synchronizations so that you can define meta-operations for CDR.

For example, you can define a sequence to push code from staging to production hosts, stop, cutover, and start a service. A sequence is defined in two parts: the properties of the sequence itself (name, user groups, and so forth) and the steps of the sequence.

Figure 12-12: Example Deployment Sequence



Defining a Sequence

Perform the following steps to define a sequence:

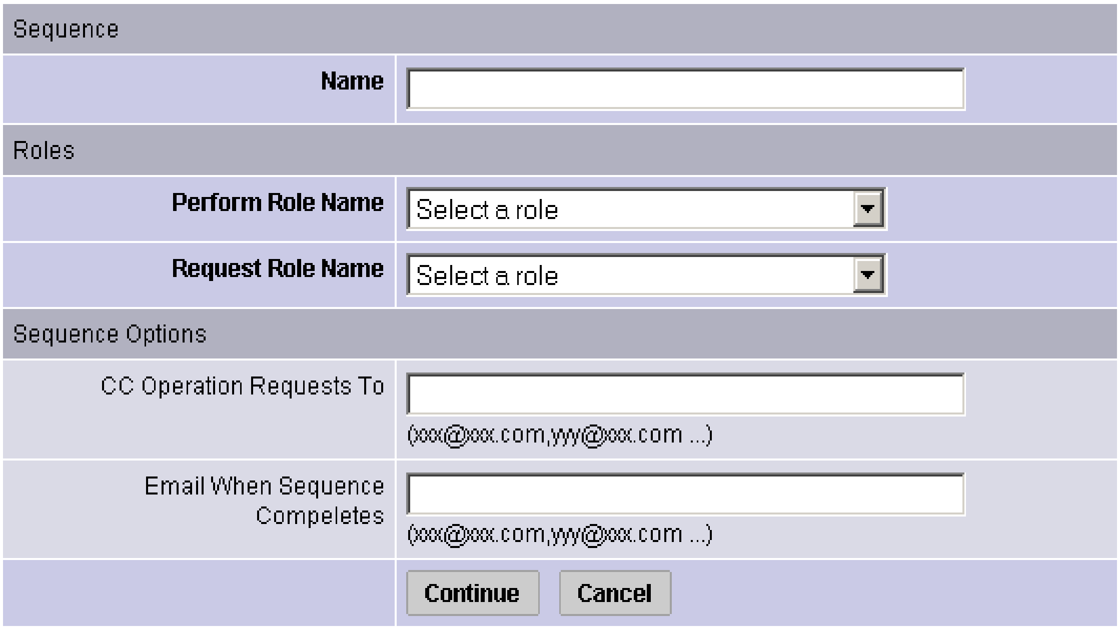
1. Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.

2. Click the Sequence Management option.

3. Click the Create a New Sequence option.

   CDR displays a page on which you specify the name of a new sequence, the user groups for the performer and requester for this sequence and email information. See Figure 12-13.

Figure 12-13: Define Sequence Page



Sequence

Name

Roles

Perform Role Name: Select a role

Request Role Name: Select a role

Sequence Options

CC Operation Requests To
(xxx@xxx.com,yyy@xxx.com ...)

Email When Sequence Compeletes
(xxx@xxx.com,yyy@xxx.com ...)

4 Specify the name of the sequence, choosing a name that users can identify with the corresponding operation that this sequence will perform, for example, Push Code to Production.

5 In the Roles section, specify the CDR user groups that you want to allow to perform or request execution of the specific sequence. The Perform Role name determines the user group whose members can perform or request that select members of your staff, or your Operations Center, perform this sequence. The Request Role Name specifies user groups whose members can request a sequence.

See “Setting up Access Control for CDR” on page 366 in this chapter for information about a description of CDR user groups that you can specify for the Perform Role and Request Role Names.

6 In the Sequence Options section, specify any email addresses to whom you want to send sequence operation requests.

7 You can also specify email addresses to which notifications can be sent when the sequence is performed and completed. The email contains the status of each step of the sequence that was performed and an indication if it ran successfully.

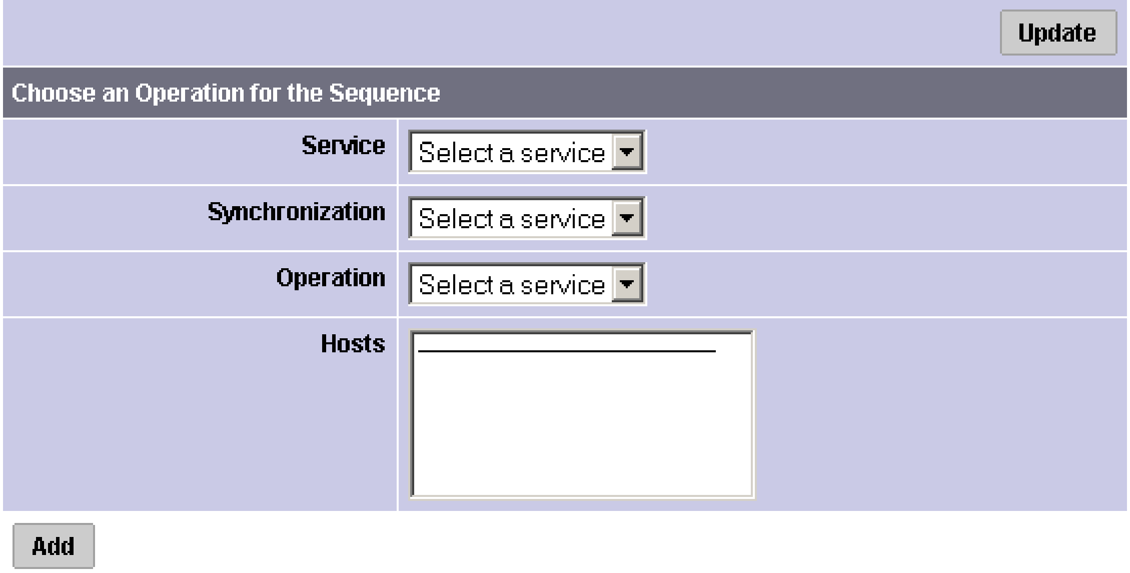
8 Click the Continue button to save the sequence properties.

To save defined sequences, you must provide entries for the Sequence Name, Perform Role, and Request Role fields.

9 A small window popsup on your screen. Use this window to select the operations to add to the sequence. First select the name of the service that you want to operate on in the Service Name drop down menu. See Figure 12-14.

If you use a pop-up blocker, this window will not pop up. You can access it by clicking the hyperlinked word popup in the sentence that says, "Add new operations with the popup window."

Figure 12-14: Sequence Operation Selection Window



Choose an Operation for the Sequence

Service	Select a service
Synchronization	Select a service
Operation	Select a service
Hosts	

10 To add services or synchronizations to a sequence:

- In both cases, first select a service from the Service drop-down menu, then select a service from the Synchronization drop-down menu.
- To add a synchronization operation, select Synchronize to Update or Synchronize To Live from the Operation drop-down menu, then select one or more destination hosts

for the synchronization from the Hosts select box. Finally, click the Add button. The information about the newly added step appears in the main window.

- To add a service operation, select None from the Synchronization drop-down menu. Then, select the name of the service operation that you want to add from the Operation drop-down menu, and select the hosts that you want to perform the service operation on in the Hosts select box. Finally, click the Add button. The information about the newly added step appears in the main window.

11 Click the Save button to save the sequence.

Modifying a Sequence

Occasionally, you need to modify an existing sequence, for example, to change assigned hosts in a step, add a step, or make other changes to attributes of the sequences.

Perform the following steps to modify a sequence:

1 Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.

2 Click the Sequence Management option.

3 Click the Modify an Existing Sequence option.

4 Click the hyperlinked name of the sequence that you want to modify.

5 Update the field entries that you want to modify and then click Continue.

6 Edit any of the sequence steps that you want.

7 Click Save to save the changes.

Deleting Sequences

CDR also allows you to delete sequences and remove their stored definition from the Model Repository.

Perform the following steps to delete a sequence:

1 Click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.

2 Click the Sequence Management option.

3 Click the Delete a Sequence option.

4. Select the check boxes next to the sequences that you want to delete and click Delete.

   CDR prompts you to confirm the deletion.

5. Click OK. CDR removes the sequences that you chose to delete.

Deleting sequences has no impact on defined services or synchronizations.

Verifying and Troubleshooting CDR Configuration

After you set up all the CDR services and synchronizations required for your site, and perform all other setup required on host machines in either your development environment or the Opsware managed environment, verify operation of the complete configuration.

The following list provides the steps to follow to verify your CDR configuration:

1. Login to the Opsware Command Center with permissions to perform service operations and synchronizations.
2. If necessary, click the Code Deployment link in the navigation panel to expand the list of CDR options and select a customer, if necessary.
3. Modify files in your staging host's Update (source) directory to enable testing synchronizations.
4. Perform all defined synchronizations. After completing the synchronizations, verify that the files, which were modified on your staging source host, were modified correctly in the directories of each destination host.
5. Perform all service operations for each defined service to verify the operations of scripts for starting, stopping, cutting over, backing up, restoring, and rolling back updates. Also, verify that all pre- and post-operations were successful.
6. Verify any sequences that you defined, executing each sequence and then checking that the operations complete successfully.

Chapter 13: Configuration Tracking Setup

IN THIS CHAPTER

This chapter discusses the following topics:

Overview of Configuration Tracking

The Configuration Tracking feature of Opsware SAS allows you 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. You use configuration tracking policies to identify the files to be tracked and actions to be taken when change is detected. A configuration tracking policy consists of one or more configuration tracking policy entries that specifies the configuration file, directory of configuration files, or configuration database that you want to track.

The Configuration Tracking feature is designed for flexibility. For example, you can set configuration tracking defaults for a node that contains a particular software application, and all servers attached to that node automatically get those defaults. You can also quickly deploy the common configuration tracking defaults to a large number of servers in your Opsware managed environment or create a specific policy for a single server.

Configuration Tracking allows you to recover from many problems caused by changes to configuration files. Using Automated Configuration Tracking, you can identify which tracked configuration files have changed, thus helping you identify the potential source of a problem. If you back up your configuration files with the Configuration Tracking feature, you can quickly restore the changed configuration files to a previous version.

You can also view a detailed history of all backup activity. This history includes a list of all tracked files that have been backed up and what types of backups occurred. If the backed up configuration files are text-based, you can download the files from the backup history and compare them to determine what specific changes have been made.

The Configuration Tracking feature is not a general-purpose backup solution. Configuration Tracking is designed to monitor text-based configuration files and specific types of configuration databases. The number and size of files that can be monitored on any managed server is limited.

File Types Supported

You can use the Configuration Tracking feature with the following types of files:

- Text-based configuration files
- The COM + Registration Database (Windows 2000)
- The IIS Metabase
- Windows Registry keys

How Change Is Detected

All servers that Opsware SAS manages have an Opsware Agent installed on them. On servers that use Configuration Tracking, every four hours the Opsware Agent inspects the configuration files and databases that you select to track.

The Opsware Agent computes an MD5 checksum to determine if the contents of a tracked file have changed. (Any change to the contents of the file results in a change to the MD5 checksum.) If the contents of the file have changed, the action that you specify in the tracking policy is performed. For example, if you create an entry in your tracking policy for the `/etc/passwd` file and select backup as the action to be taken, the file is backed up when the Opsware Agent discovers a change in the `/etc/passwd` file.

The creation or deletion of a tracked file (or files inside a tracked directory) also counts as change and triggers a policy's action. (There are some exceptions; See "Special Considerations for Directory and Wildcard Targets" on page 395 in this chapter for more information.)

Changes to the properties of a tracked file or directory (such as changes to permissions or timestamps) do not count as a change. When a file or directory is backed up, however, its properties are backed up as well.

The first time that a tracking policy is deployed, all targets are considered changed. The Opsware Agent is encountering the files for the first time, and all of the policy's actions are triggered.

Types of Actions Performed

Opsware SAS can perform the following actions when change is detected in a tracked configuration file or configuration database:

- Back up
- Send email to addresses specified in the policy entry
- Send email to a designated notification group specified by a custom attribute
- Create an entry in the server's standard system log (The syslog on Unix servers and the event log on Windows servers)

Types of Backups Performed

If you selected backup as the action for a tracked configuration file, the two general types of backups that can occur are incremental backups and full backups.

Incremental Backups

During an incremental backup, only targets that have changed since the last backup (and that have been selected to be backed up) are backed up.

An incremental backup occurs automatically when the Opsware Agent detects change in a tracked file that is selected to be backed up. (The Opsware Agent checks for change every four hours.)

Incremental backups also occur before and after you restore a previous version of a backed up configuration file to a server. These backups allow you to roll back the restored files.

Full Backups

During a full backup, all tracked configuration files that were selected to be backed up are backed up, not just the files that have changed.

Once a week, the Opsware Agent on a server checks to see if any files have changed since the last full backup. If any files have changed, Opsware SAS performs a new full backup. If no files have changed, the full backup does not take place.

You can also force Opsware SAS to perform a full backup on a server by selecting the *Perform Manual Backup* option. (See the *Opsware® SAS 5.2 User's Guide* for more information about Performing Manual Backups.)

See the *Opsware® SAS 5.2 User's Guide* for more information about Backup types.

Backups are stored in the Software Repository until you delete them. You should delete old backups periodically, especially if you are backing up a large number of files that change frequently. See the *Opsware® SAS 5.2 User's Guide* for more information about the procedure for deleting backups. See the *Opsware® SAS 5.2 Administration Guide* for information about mass deletion of backup files.

Email Automated Configuration Tracking and Logging Actions

You can choose to have email sent when a monitored target changes. The following example shows the text of an email generated when a tracked file changed.

```
From: <configurationtracking@yourcompany.com>
Date: Thu Jan 16, 2003  5:40:11 PM US/Pacific
To: <joe@yourcompany.com>
Subject: athena.cust.com: Configuration Tracking CHANGE
notification
Configuration Tracking has detected a CHANGE event
Host: athena.cust.com
Object: /db/file1l1
```

The email specifies the name of the server and the name of the object that changed. The object can be a file, a directory, or a configuration database.

If you are monitoring a directory target, you receive email about the directory itself and about changes to the files in the directory (except when a file is deleted.) For example, if three new files are created in a directory, you would receive four emails, one for the directory and three for the new files.

If you selected the logging action, an entry is made to the server's standard system log when a change is detected. You select the type of log entry that you want to have written. Opsware SAS uses three standard entry types:

- Info
- Warning
- Error

How the entry types are identified is system-dependent. For example, on most systems Warning entries are identified by the word warning. In some systems, however, a number is used to identify the log entry type.

The following example shows a warning log entry written on a Solaris Server:

```
Jan  8 00:05:25 athena.cust.com Configuration Tracking:
[ID702911
local0.warning] Configuration Tracking: /other/otherfile1 :
Event CHANGE occurred
Jan  8 00:05:25 athena.cust.com Configuration Tracking: [ID
702911
local0.warning] Configuration Tracking: /other/otherfile1 :
Event CHANGE occurred
```

Creating the Email Notification List

Sending email to a server's backup notification list is one of the actions that you can select in a tracking policy entry. The email notification list is a list of email addresses that you define for the following custom attribute:

```
   backup_notification_email
```

This attribute can be set on the server itself or on the customer to which the server is attached. Setting the attribute at the customer node level allows you to use the same email notification list for all servers that belong to the same customer (assuming that these servers have all been attached to the same customer and do not have the `backup_notification_list` attributes set on the servers themselves).

Search Order for Email Notification List Attribute

On a server that has a policy that includes the Email Notification List for Server action selected, the server searches for the `backup_notification_email` attribute in the following order:

- Server
- Customer

After the custom attribute is found, its value is used (for example, the email address of the notification list) and the search is concluded. If, for example, the backup_notification_ email attribute is set on a server, the server's email notification list is used, even if the server is assigned to a customer that has a different `backup_notification_email` attribute.

Format of Email Notification List

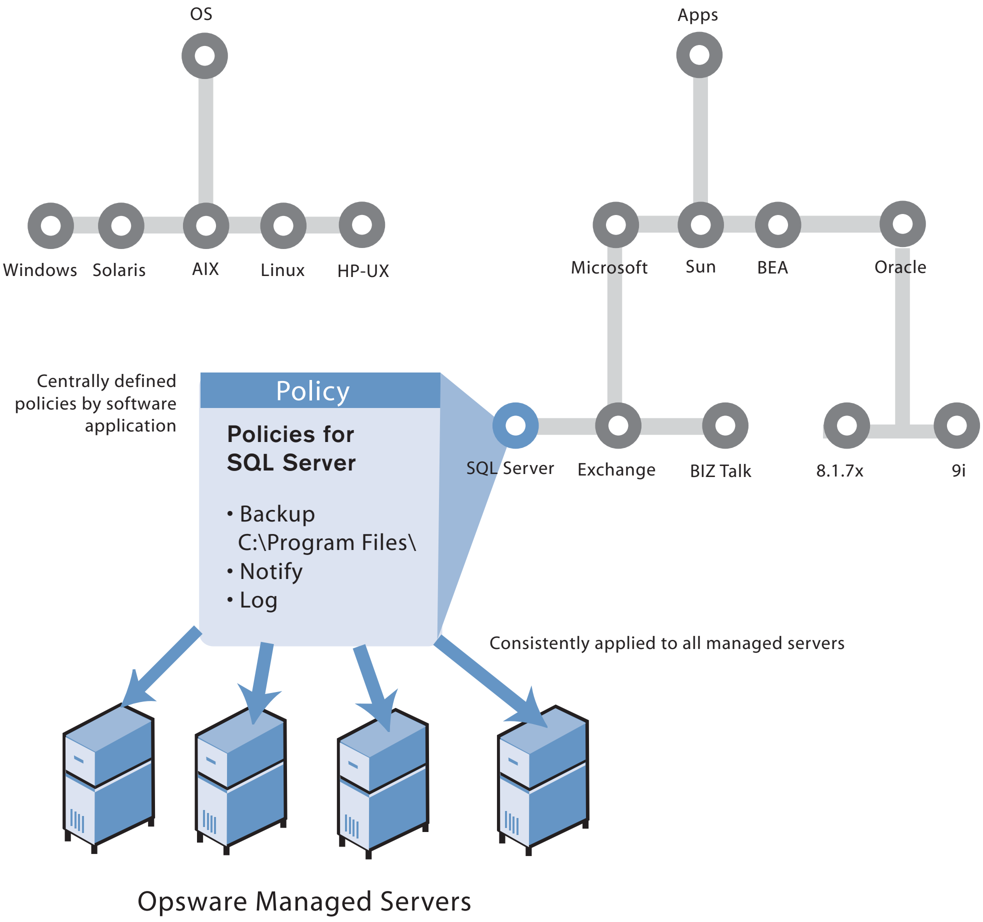
The notification list can contain multiple email addresses. The email address must be formatted as a comma-separated list.

Configuration Tracking Policies

You use configuration tracking policies to specify which files and configuration databases to monitor for change and what actions to take when change is detected.

A configuration tracking policy consists of one or more configuration tracking policy entries. You create one entry for each target that you want to track. The target specifies the configuration file, directory of configuration files, or configuration database that you want to track. In the case of directories and files, the target is the fully qualified path of the directory or file (unless you are using wildcards). You then specify the action to be taken when change to the target is detected. See Figure 13-1.

Figure 13-1: Configuration Tracking Policy



The combination of all the individual tracking policy entries for a server is referred to as a server's configuration tracking policy, and the combination of all the tracking policy entries for a node is referred to as a node's configuration tracking policy (for example, the tracking policy is the combination of tracking policy entries).

Methods for Creating Tracking Policies

You can create tracking policies in two ways:

- By using Opsware nodes (See "Node-Based Tracking Policies" on page 398 in this chapter for more information.)
- By creating custom tracking policies for a selected server or set of servers (See the *Opsware® SAS 5.2 User's Guide* for more information.)

The preferred way to create a tracking policy is by using Opsware nodes. Among other functions, an Opsware node specifies what software should be installed on the servers that are attached to that node. For example, if a server is assigned to a Sun ONE Web Server node, the software packages associated with that node are installed on the server when the server is reconciled.

Because the node specifies which software packages to install, the tracking policies for the software packages' configuration files are usually created as part of the node.

Configuration Tracking Policy Targets and Wildcards

If you selected a file or directory as the target type, the target can include wildcards (* to match 0 or more characters, and ? to match a single character). Wildcards cannot be used with other types of targets.

Wildcards used in file targets produce different results than wildcards used in directory targets.

- If you use wildcards in a file target, Opsware SAS searches for files that match the pattern that you specify.
- If you use wildcards in a directory target, Opsware SAS searches for directories that match the pattern that you specify. The contents of all the matching directories are tracked.

If you selected the "include subdirectories option," the contents of all the subdirectories of all matching directories are also tracked.

Wildcards can be used in any part of the path that you specify in the target (except for the drive letter.) Wildcards used in the target field behave exactly as they do on the selected operating system.

Special Considerations for Directory and Wildcard Targets

In most cases, the Configuration Tracking feature is used to track specific files. Specific files are tracked when you select the File target type and supply the fully qualified path of the filename without using wildcards. (Tracking configuration databases, such as the Windows COM+ Registration Database, also counts as tracking specific files.)

Because the tracking feature is designed to monitor files that you are specifically interested in (for example, configuration files), tracking specific files is the recommended way to use the feature. When you monitor a specific file, Opsware SAS is able to keep a more complete record of the file; Opsware SAS can, for example, note that the file does not exist on the server.

If you do not know the fully qualified path of a configuration file, you can choose to monitor directories or use wildcard targets. This option is useful in some circumstances, such as when an application dynamically creates configuration files and it is not possible to know the file names in advance. The next sections explain special considerations that apply if you monitor directories or use wildcard targets.

Tracking the Contents of a Directory

The following conditions apply when you select the Directory target type. These conditions apply whether or not you use any wildcards in your target.

- You cannot use the Configuration Tracking feature to delete files that were created in monitored directories. Because Opsware SAS was not tracking the file specifically, Opsware SAS did not note the file's absence and cannot restore the file to a state before it existed.
- When a specific tracked file is deleted, your selected action is triggered for the file. If a file is deleted inside a monitored directory, the action is triggered only for the directory object and not for the file itself. For example, you have selected the email action, you would receive email that the directory has changed, but you would not receive email about the specific file. (You do receive email about files created inside monitored directories.)
- If you are monitoring a directory tree (by selecting the include subdirectories option), actions are triggered for the file, the file’s directory, and all of the parent directories up to the directory specified in the target.

Tracking Files through Wildcard Targets

The following conditions apply only when you select the File target type *and* use wildcards in the target:

- When a file is created that matches a wildcard target, the creation of the file is noted and your selected action is triggered. The fact that the file did not previously exist, however, was not noted, and no entry was created in the backup history about the file's absence. This file cannot be deleted by using the Configuration Tracking feature.
- When a file tracked through a wildcard target is deleted, no action is taken.

Directories Tracked by Wildcard Targets

The conditions discussed in this section apply to directory objects when you select the Directory target type and use wildcards in the target.

The contents of directories tracked by wildcard targets are subject to the same conditions as the contents of directories that are fully specified (for example, not found as a result of a wildcard search). The directory objects tracked through wildcard targets, however, are not tracked in the same way as directory objects with fully specified targets. The following differences apply:

- If you track a specific directory and the directory does not exist on a server, the absence of the directory triggers the action you selected. An entry is made in the backup history about the absence of the directory and this entry can be used to delete the directory. No such entries are made for directories tracked through wildcard targets.
- The deletion of a directory found by a wildcard target does not trigger an action. The creation of a directory that is found by a wildcard target, however, does trigger an action.
- If you are monitoring a directory tree through a wildcard target and any subdirectory is deleted, your selected action is triggered for all the directory's parent directories, up to the directory specified in the target. When subdirectories are created, however, your selected action is triggered both for the top-level directory and for the specific subdirectories.

Configuration Tracking Policy Limits

Because Configuration Tracking is not a general-purpose backup solution, Opsware SAS enforces limits on the number of objects that can be monitored. The limits help keep backup volume from growing too large; excessive backup volume can degrade system performance.

You should also periodically delete backups; See the *Opsware® SAS 5.2 User's Guide* for more information about Deleting Backups. See the *Opsware® SAS 5.2 Administration Guide* for information about mass deletion of backup files.

The limits apply to the number and size of objects that can be monitored. In this context, *objects* are files or configuration databases and the directories that make up the path to a file. For example, if you set up a policy entry to track the contents of the `/etc/init` directory and the directory contains 10 files, the policy entry is tracking 12 objects (the 10 files plus the `/etc and /init` directories). Similarly, if you set up a policy entry to track the `/etc/system` file, the policy entry is tracking 2 objects (the `/etc` directory and the system file).

The following limits apply to the number of objects that can be tracked and to the size of files that can be tracked:

- No more than 2500 objects can be tracked on a single server (for example, the server's aggregate tracking policy, which is the combination of all its tracking policy entries, cannot cause more than 800 objects to be tracked.)
- The total number of objects tracked by a single tracking policy entry cannot be larger than 250. (A tracking policy entry is a single item in a tracking policy.)

  For example, if you create a tracking policy entry to monitor the contents of the `/etc/init` directory, and the directory contains 250 files, you have exceeded the limit for a single tracking policy entry. Because the `/etc` and `/init` directories count as objects, the total number of objects monitored by this policy entry exceeds the limit of 250.
- Files greater than 2 megabytes cannot be monitored.

The target you specify in a tracking policy entry can contain wildcards. Exercise caution in using wildcards, because wildcards can cause a large number of files to be monitored.

If you exceed any of these limits, you receive an error message when you attempt to deploy the server's tracking policy, and the deployment fails. See “Deploying Tracking Policies” on page 402 in this chapter for more information.

If a policy exceeds any of these limits after the policy is deployed on a server, no further actions are triggered on that server. Backups, for example, stop taking place. When any limit is exceeded after a policy is deployed, a warning email is sent to the following addresses:

- An administrator's email address that is specified during installation. The email address is referred to as the error email address.
- The server's backup notification email list.

See “Ways to Use Opsware SAS Configuration Parameters” on page 18 in Chapter 2 for more information.

If the server does not have a backup notification list assigned to it, the warning message is sent only to the error email address.

Node-Based Tracking Policies

This section provides information on node-based tracking policies within Opsware SAS and contains the following topics:

- Overview of Node-Based Tracking Policies
- Creating Node-Based Policy Entries
- Deploying Tracking Policies
- Reconciling a Node’s Configuration Tracking Policy
- Viewing a Node’s Tracking Policy
- Editing a Node’s Configuration Tracking Policy
- Editing a Node’s Configuration Tracking Policy Entry
- Disabling a Node’s Configuration Tracking Policy Entries
- Deleting an Entry in a Node’s Configuration Tracking Policy
- Re-enabling a Tracking Policy Entry

Overview of Node-Based Tracking Policies

You create a node’s tracking policy by creating one or more tracking policy entries. After you create a node’s policy, you can edit the individual policy entries, you can disable individual policy entries, and you can add new policy entries.

You create nodes by creating child nodes from parent nodes. The child nodes inherit the software policies of their parents. The same principle applies to tracking policies. If the parent node has a tracking policy defined for it, all the node’s children inherit the tracking policy. If you make changes to a node's tracking policy, the node's children also inherit the changes.

See “Managing Nodes on the Software Tree” on page 255 in Chapter 10 for more information.

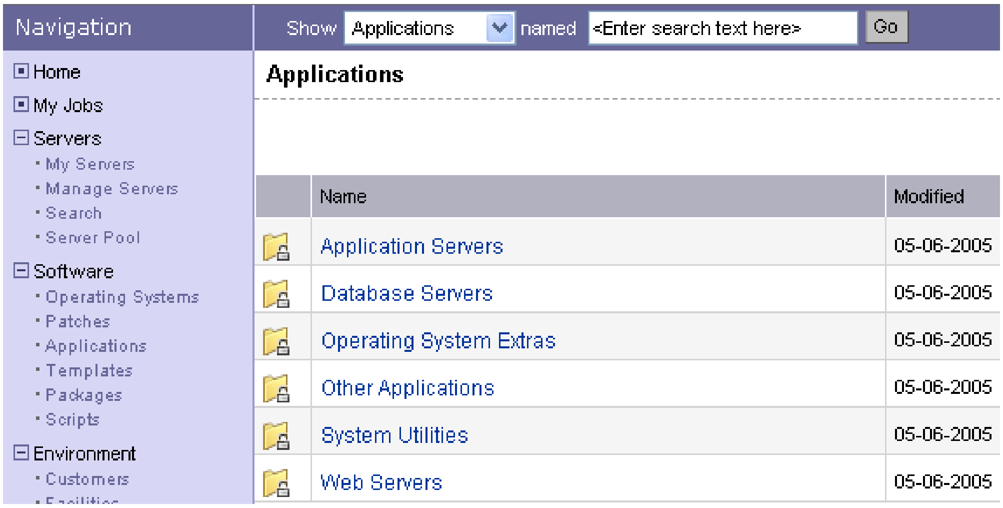
You can, however, disable all or part of any inherited tracking policy in a child node.

Creating Node-Based Policy Entries

Perform the following steps to create the tracking policy for an existing Opsware node:

1. From the navigation panel, click Software and then select the relevant type of software (for example, patches, applications, and so forth), as Figure 13-2 shows.

Figure 13-2: Selecting Node Types



Navigation

- ⊡ Home
- ⊡ My Jobs
- ⊟ Servers
  - My Servers
  - Manage Servers
  - Search
  - Server Pool
- ⊟ Software
  - Operating Systems
  - Patches
  - Applications
  - Templates
  - Packages
  - Scripts
- ⊟ Environment
  - Customers
  - Facilities

Show Applications named <Enter search text here> Go

Applications

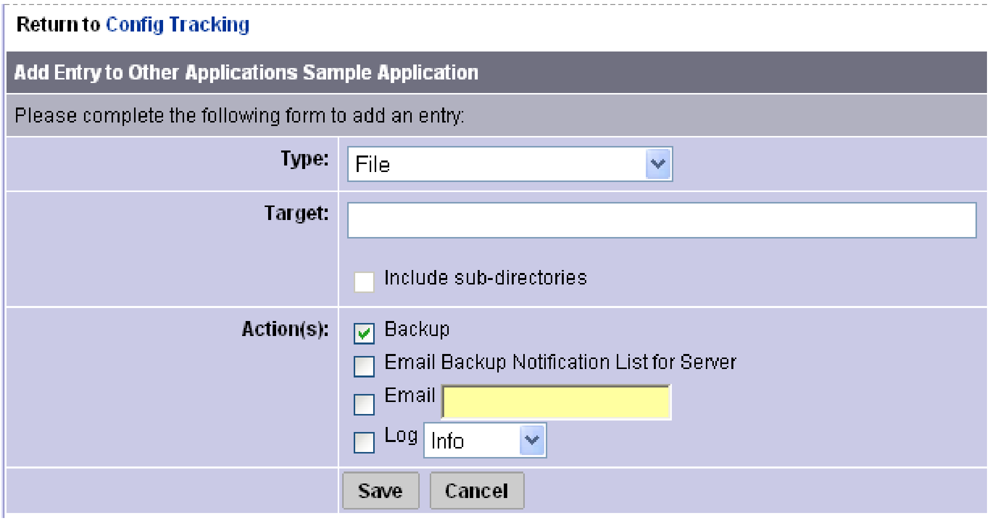
	Name	Modified
	Application Servers	05-06-2005
	Database Servers	05-06-2005
	Operating System Extras	05-06-2005
	Other Applications	05-06-2005
	System Utilities	05-06-2005
	Web Servers	05-06-2005

2. Navigate to the node for which you want to create a tracking policy.

3. Click the Config Tracking tab.

4 Click Add Entry. The Track Configurations: Add Entry page appears, as Figure 13-3 shows.

Figure 13-3: Track Configurations: Add Entry



Return to Config Tracking

Add Entry to Other Applications Sample Application

Please complete the following form to add an entry:

Type:	File
Target:	 □ Include sub-directories
Action(s):	☑ Backup □ Email Backup Notification List for Server □ Email □ Log Info

5 Select the type, define the target (when appropriate), and select the actions that you want to take place when a change in the configuration file or database is discovered. Table 13-1 describes each of the selections that you must make.

Table 13-1: Add Entry: Configuration Tracking

FIELD	DESCRIPTION
Type	**File**: monitor the file specified in the target field **Directory**: monitor all the files in the directory specified in the target field. The following types are available only for Windows servers. **Windows Registry**: specify key in target field **IIS Metabase**: entire Metabase is monitored; do not specify target **COM + Registration Database**: entire Registry is monitored; do not specify target

Table 13-1: Add Entry: Configuration Tracking

FIELD	DESCRIPTION
Target	If you selected the file type, specify the full path (including the drive letter on Windows servers) of the file that you want to monitor. If you selected the directory type, specify the full path of the directory (including the drive letter on Windows servers) that you want to monitor. You also have the option of monitoring subdirectories. (Select the “Include Subdirectories” check box.) If you select the file or directory type, you can use wildcards in the target. (See “Configuration Tracking Policy Targets and Wildcards” on page 394 in this chapter for more information.) If you selected the Windows Registry type, specify the Windows registry key. This key and all its subkeys are backed up. Use standard syntax for Windows Registry keys (For example, `HKEY_LOCAL_MACHINE\SOFTWARE)` If you selected the IIS Metabase or COM + Registration Database type, do not specify the target.
Actions (you can select multiple options)	**Backup**: back up the specified file, directory, COM + Registration Database, Windows Registry keys, or IIS Metabase. **Email Backup Notification List for Server**: send an email to the backup notification list for the selected server. See “Creating the Email Notification List” on page 391 in this chapter for more information. **Email**: send an email to the address or addresses specified in this field when a change is detected. Use a comma-separated list for multiple email addresses. (Not available for Windows Registry.) **Log**: add an entry to the server’s system log when a change is detected. You can choose to write the following types of log entries to the server’s system log: Info Warning Error

6. Click Save to add the entry to the tracking policy.
7. If you want to continue to add entries to the tracking policy, click Add Entry and repeat this procedure.

You must perform a Configuration Tracking reconcile to deploy the tracking policy to the appropriate servers.

See “Reconciling a Node’s Configuration Tracking Policy” on page 402 in this chapter for more information.

Deploying Tracking Policies

Tracking policies are not deployed to your servers until you perform a configuration tracking reconcile. (This is not the same as software reconcile). See “Reconciling a Node’s Configuration Tracking Policy” on page 402 in this chapter for information about the procedures for performing configuration tracking reconciles.

Reconciling a Node’s Configuration Tracking Policy

You must perform a configuration tracking reconcile to apply the node's tracking policy to the servers attached to the node. You must do this when you create a policy, when you make any changes to a policy, or when you attach or detach a server from a node.

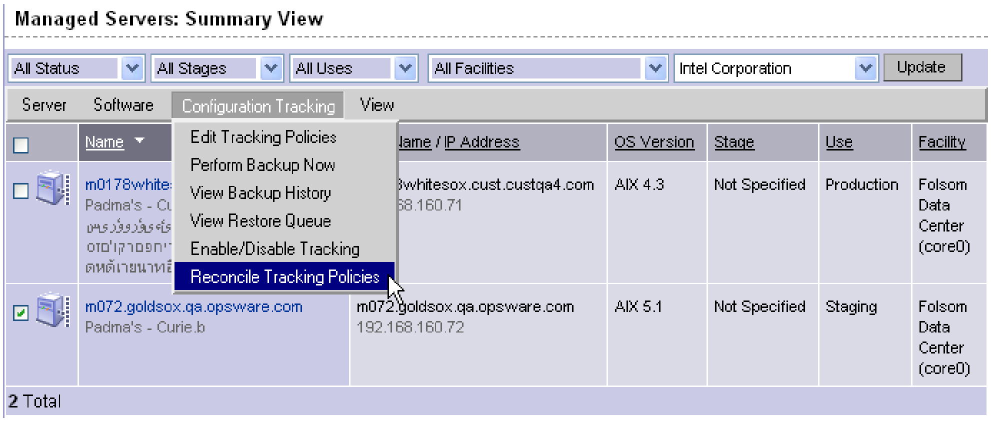
Performing a configuration tracking reconcile on a server also automatically enables the Configuration Tracking feature on that server.

Perform the following steps to perform a reconcile for a node-based configuration tracking policy:

1. From the navigation panel, click Software and then select the relevant type of software (for example, patches, applications, and so forth).
2. Navigate to the node whose tracking policy you want to reconcile.
3. Click the Members tab. A list of the servers attached to the node displays.
4. Select the servers whose tracking policy you want to reconcile. (You can select the check box at the top of the list to select all the servers in the list.)

5 Under the Configuration Tracking drop-down menu, select “Reconcile Tracking Policies,” as Figure 13-4 shows.

Figure 13-4: Reconcile Tracking Polices



☐	Name	ame / IP Address	OS Version	Stage	Use	Facility
☐	m0178white Padma's - Cu [illegible]	8whitesox.cust.custqa4.com 68.160.71	AIX 4.3	Not Specified	Production	Folsom Data Center (core0)
☑	m072.goldsox.qa.opsware.com Padma's - Curie.b	m072.goldsox.qa.opsware.com 192.168.160.72	AIX 5.1	Not Specified	Staging	Folsom Data Center (core0)

2 Total

At this point, Opsware SAS performs a test reconcile to ensure that the reconcile can be performed without errors. The progress of the test reconcile process displays. Click the View Details button if you want to see information about what changes will be made when the reconcile is performed.

6 If the test reconcile is completed without errors, click Reconcile.

The progress of the reconcile process displays. Click View Details if you want to see information about what changes were made during the Reconcile process.

Viewing a Node’s Tracking Policy

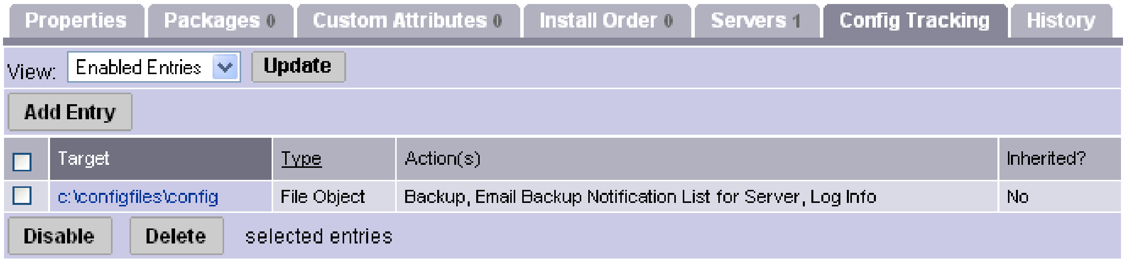
Perform the following steps to view a node's tracking policy:

1 From the navigation panel in the Opsware Command Center, click Software then select the type of software.

2 Navigate to the node whose tracking policy you want to examine.

3. Click the Config Tracking tab. The entries that make up the tracking policy for the node display. You can verify that an entry in a tracking policy was inherited by looking at the Inherited field, as Figure 13-5 shows.

Figure 13-5: Viewing a Node's Configuration Policy



□	Target	Type	Action(s)	Inherited?
□	c:\configfiles\config	File Object	Backup, Email Backup Notification List for Server, Log Info	No

Tracking policy entries are identified by target. If a node inherits two or more policy entries from its parent nodes that have the same target, these entries display as a single entry when you view the child's and node's tracking policy. The single entry, however, combines all of the actions that you selected for the target.

If the child also has a policy entry for the same target, the child's policy displays as a separate entry. For example, if a child node inherits three policy entries from its parents for the `/etc/passwd` target and the child also has its own policy entry for `/etc/passwd`, two entries display when you view the child's policy.

Editing a Node's Configuration Tracking Policy

You can edit tracking policy entries in the following ways:

- You can make changes to tracking policy entries that are not inherited from another node. For example, if the policy entry specifies that a configuration file should be backed up, you can add an action, such as sending an email when a change is noticed.
- You can disable a tracking policy entry that has been inherited from another node. (You cannot delete an inherited tracking policy.)
- You can delete a tracking policy entry that is not inherited. After an entry is deleted, it cannot be undeleted. (You cannot disable a tracking policy that is not inherited.)
- You can re-enable a previously disabled tracking policy entry.

If the node has any child nodes, the child nodes inherit all the changes that you make to the parent node.

When you make a change to a node's tracking policy, that change is not immediately made on the servers attached to the node. You must perform a tracking policy reconcile for the changes to take effect.

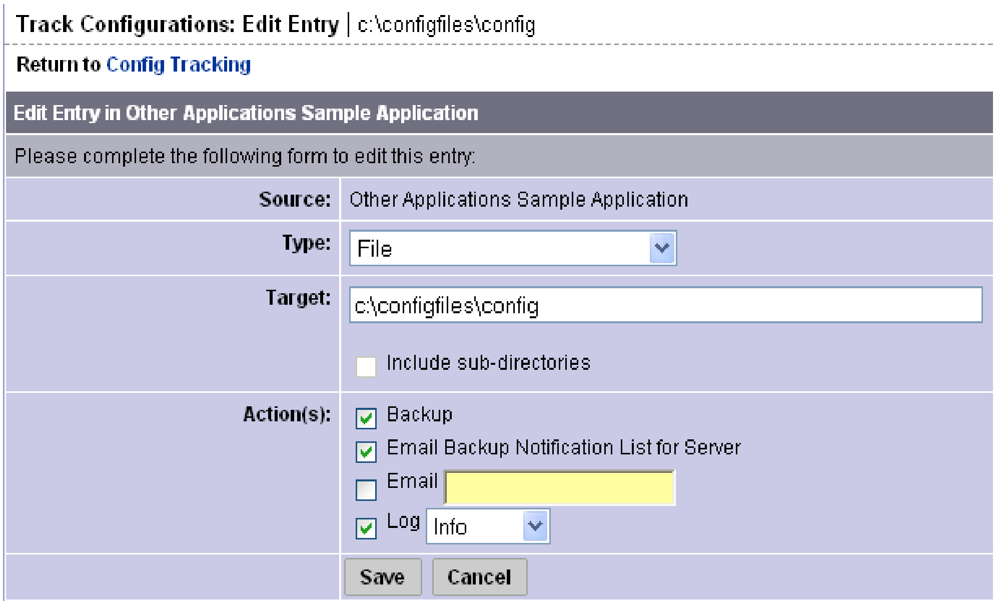
Editing a Node's Configuration Tracking Policy Entry

You can make changes only to tracking policy entries that are not inherited from other nodes.

Perform the following steps to edit a node's tracking policy:

1. From the navigation panel, click Software and then select the relevant type of software (for example, patches, applications, and so forth).
2. Navigate to the node that has the tracking policy entries that you want to edit.
3. Make sure that enabled entries display. If disabled entries display, choose enabled entries from the View drop-down menu and then click Update.
4. Click the link in the target field for a non-inherited policy entry that you want to edit. The Edit Entry page appears, as Figure 13-6 shows.

Figure 13-6: Track Configurations: Edit Entry Page



Track Configurations: Edit Entry | c:\configfiles\config

Return to Config Tracking

Edit Entry in Other Applications Sample Application

Please complete the following form to edit this entry:

Source:	Other Applications Sample Application
Type:	File
Target:	c:\configfiles\config □ Include sub-directories
Action(s):	☑ Backup ☑ Email Backup Notification List for Server □ Email ☑ Log Info

5. Make the desired changes to the tracking policy entry. You can change the type, change the target, clear existing actions, and select new actions.

6. Click Save to commit the changes.

   You are returned to the tracking policy page for the selected node.

You must perform a configuration tracking reconcile to deploy the changes to the appropriate servers.

Disabling a Node’s Configuration Tracking Policy Entries

You can only disable inherited tracking policy entries.

Perform the following steps to disable policy entries:

1. From the navigation panel, click Software and then select the relevant type of software (for example, patches, applications, and so forth).
2. Navigate to the node that has the tracking policy entries that you want to disable.
3. Make sure that enabled entries display. If disabled entries display, select enabled entries from the View drop-down menu, and then click Update.
4. Select the inherited tracking policy entry or entries that you want to disable. You can select all displayed entries by clicking the first check box in the list.
5. Click the Disable button.
6. Click the Disabled Entries button to commit the changes.

You must perform a configuration tracking reconcile to deploy the changes to the appropriate servers.

Deleting an Entry in a Node’s Configuration Tracking Policy

You can only delete tracking policy entries that are not inherited.

Perform the following steps to delete policy entries:

1. From the navigation panel, click Software and then select the relevant type of software (for example, patches, applications, and so forth).
2. Navigate to the node that has the tracking policy entries that you want to delete.

3. Make sure that enabled entries display. If disabled entries display, select enabled entries from the View drop-down menu, and then click Update.
4. Select the (non-inherited) tracking policy entry or entries that you want to delete. You can select all displayed entries by clicking the first check box in the list.
5. Click the Delete button.
6. Click Delete Entries button to commit the changes.

You must perform a configuration tracking reconcile to deploy the changes to the appropriate servers.

Re-enabling a Tracking Policy Entry

Perform the following steps to re-enable a disabled tracking policy entry:

1. From the navigation panel, click Software and then select the relevant type of software (for example, patches, applications, and so forth).
2. Navigate to the node that has the tracking policy entries that you want to enable.
3. Select disabled entries from the drop-down box and then click Update to display the disabled entries.
4. Select the disabled tracking policy entry or entries that you want to enable. You can select all displayed entries by clicking the first check box in the list.
5. Click the Enable button.
6. Click the Enabled Entries button to commit the changes.

You must perform a configuration tracking reconcile to deploy the changes to the appropriate servers.

Appendix A: Permissions Reference

IN THIS APPENDIX

This appendix discusses the following topics:

- Permissions Required for Opsware Tasks
- Permissions Required for the OCC Client
- Script Execution Permissions
- Predefined User Group Permissions
- Code Deployment User Groups

Permissions Required for Opsware Tasks

The following table lists the feature permissions according to tasks that can be performed with the Opsware Command Center.

Table 1: Permissions for Opsware Tasks

TASK	REQUIRED PERMISSION
OS PROVISIONING	
Prepare OS	Wizard: Prepare OS
Edit OS nodes	Operating Systems
Install OS	Wizard: OS Provisioning
View servers in the server pool	Server Pool
View and edit templates	Templates
SOFTWARE PROVISIONING	
Manage (upload, delete, deprecate) packages	Packages
Search for or view packages	Packages

Table 1: Permissions for Opsware Tasks

TASK	REQUIRED PERMISSION
Manage (create, edit, delete) software nodes	Model: Applications
Assign software nodes	Manage Servers and Groups
Reconcile a server	Wizard: Install Software Wizard: Uninstall Software Wizard: Reconcile
Install templates	Templates
Manage (create, edit, delete) templates	Templates
PATCH MANAGEMENT	
Set up the patch management system	Patches
Upload patches	Patches Wizard: Upload Patch
Edit patch properties, mark as available	Patches
Install available patches	Wizard: Install Patch
Install untested patches	Patches Wizard: Install Patch
Uninstall patches	Wizard: Uninstall Patch
Run Microsoft update	Wizard: Microsoft Patch Update
View patches (link in navigation panel)	Patches
CONFIGURATION TRACKING	
Create or edit tracking policy	Configuration Tracking Managed Servers and Groups Model: Applications
Reconcile tracking policy	Configuration Tracking Wizard: Reconcile Managed Servers and Groups Model: Applications

Table 1: Permissions for Opsware Tasks

TASK	REQUIRED PERMISSION
Perform configuration backup	Configuration Tracking Managed Servers and Groups Model: Applications
View backup history, restore queue	Configuration Tracking Managed Servers and Groups Model: Applications
Enable or disable tracking	Configuration Tracking Managed Servers and Groups Model: Applications
SERVER MANAGEMENT	
Edit server properties	Managed Servers and Groups
Edit server network properties	Managed Servers and Groups
Edit server custom attributes	Managed Servers and Groups
Deactivate server	Deactivate
Delete server	Managed Servers and Groups
Clone server	Managed Servers and Groups
Re-assign customer	Managed Servers and Groups
Re-assign node	Managed Servers and Groups
Remove node	Managed Servers and Groups
View servers (read-only access)	Managed Servers and Groups
Run server communications test	Managed Servers and Groups
Lock servers	Managed Servers and Groups
Set scheduled job to refresh server list	Allow Run Refresh Jobs
SERVER GROUPS	
Manage (create, edit, delete) and use private group	(none)
Use public group	(none)
Manage (create, edit, delete) public group	Manage Public Server Groups

Table 1: Permissions for Opsware Tasks

TASK	REQUIRED PERMISSION
Attach nodes (patches, applications, and others) to public group	Model Public Server Groups
REPORTS	
Create or view reports	Data Center Intelligence Reports
MANAGE ENVIRONMENT	
Create or edit customer	Customers
Create or edit facility	Facilities
Create or edit service level	Model: Service Levels
IP RANGES AND RANGE GROUPS	
IP Ranges	IP Ranges and Range Groups Model: Hardware Model: Opsware DNS
IP Range Groups	IP Ranges and Range Groups Model: Hardware Model: Opsware DNS
SYSTEM CONFIGURATION	
Manage users and groups	(Administrators group only)
Define server attributes	Server Attributes
Run system diagnosis tools	System Diagnosis
Manage Opsware System configuration	Configure Opsware
Run Opsware multimaster tools	Multimaster
Gateway management	Manage Gateway
OTHER TASKS	
Run custom extension	Wizard: Custom Extension
Run control scripts on Intelligent Software Modules (ISMs)	ISM Controls

Table 1: Permissions for Opsware Tasks

TASK	REQUIRED PERMISSION
Run scripts	See “Script Execution Permissions” on page 417.
Deploy code	See “Code Deployment User Groups” on page 424.

Permissions Required for the OCC Client

The tables in this section summarize the permissions required for the OCC Client features, except for Global Shell. For more information, see “Global Shell Permissions” on page 42.

Permissions Required for (ODAD)

To use ODAD in the OCC Client, you must have the permissions described in the table below.

Table 2: ODAD Feature Permissions

FEATURE	PERMISSIONS
Allow Deploy Agent	• **Yes**: Allows you to deploy (install) Opsware Agents with ODAD. • **No**: Does not allow you to deploy Agents with ODAD.
Allow Scan Network	• **Yes**: Allows you to scan the network with ODAD for servers on which to deploy Agents. • **No**: Does not allow you to scan the network with ODAD.
Managed Servers and Groups	Allows you to view and manage servers and server groups.

Permissions Required for ACM

To use ACM in the OCC Client, you must have the permissions listed in the table below. You also need access to managed servers and customers.

Table 3: ACM Feature Permissions

FEATURE	PERMISSIONS
Configuration (Application Configuration)	• **Read**: Allows you to view Application Configurations. • **Write**: Allows you to create Application Configurations. • **None**: Neither
Configuration files (Application Configuration Templates)	• **Read**: Allows you to view Application Configuration Template. • **Write**: Allows you to create Application Configuration Template. • **None**: Neither
Configuration on Servers: Pushing Application Configuration changes to a server	• **Read**: Allows you to view changes. • **Write**: Allows you to push changes. • **None**: Neither
Allow Check Consistency on Servers: Comparing a template against an actual configuration file	• **Yes**: Allows you to compare a template with an actual configuration file on a server. • **No**: Does not allow you to compare a template with an actual configuration file on a server.

Permissions Required for Server Compliance

To use Server Compliance in the OCC Client, you must have the permissions listed in the table below.

Table 4: Server Compliance Feature Permissions

FEATURE	PERMISSIONS
Manage Selection Criteria	• **Read**: Allows you to load selection criteria for a snapshot or an audit. • **Write**: Allows you to create, modify, and delete selection criteria for a snapshot or an audit. • **None**: Neither
Audit Templates	• **Read**: Allows you to view an audit template. • **Write**: Allows you to create, modify, and delete an audit template. • **None**: Neither
Audit Results	• **Read**: Allows you to view audit results. You must have read permission on the targets (servers, server groups, and snapshots) that were included in the audit process. • **Write**: Allows you to perform an audit and delete audit results. To perform an audit, you must have read permissions for all sources and targets (servers, server groups, and snapshots) that are specified in the audit template. • **None**: Neither

Table 4: Server Compliance Feature Permissions

FEATURE	PERMISSIONS
Snapshot Templates	• **Read**: Allows you to view a snapshot template. You must have read permission on all servers and server groups that the template references. • **Write**: Allows you to create, modify, and delete a snapshot template. • **None**: Neither
Manage Snapshots on Servers	• **Read**: Allows you to browse a snapshot. You must have read permission on the server where the snapshot was recorded. • **Write**: Allows you to create and delete a snapshot, and copy objects from a snapshot to a destination server. To create a snapshot, you must have read permissions for all targets (servers and server groups) that are specified in the snapshot template. To delete a snapshot, you must have permission to read it. To copy an object to a destination server, you must have write permission on that destination server. • **None**: Neither
Allow General Snapshot Management	• **Yes**: Allows you to create and delete a general snapshot. You can only create a general snapshot from a snapshot that you can read. A user that has permission to read a snapshot can also browse a general snapshot. • **No**: Does not allow you to create and delete a general snapshot.

Permission Required for Create Package

To use Create Package in the OCC Client, you must have the permission described in the table below. You also need access to managed servers.

Table 5: Create Package Feature Permission

FEATURE	PERMISSIONS
Allow Create Package	• **Yes**: Allows you to create an installable software package. • **No**: Does not allow you to create an installable software package.

Script Execution Permissions

The following table provides an overview of the most common script management and script execution tasks, and displays the permissions required to perform a task. Because each task is performed on a specific type of script (My Scripts, Shared Script, or Ad-Hoc Script), the table also lists the permissions according to the type of script.

Table 6: Permissions Required for Script Tasks

SCRIPT TASK	SCRIPT TYPE	REQUIRED PERMISSIONS FOR SCRIPT TASK AND TYPE	COMMENTS
SCRIPT MANAGEMENT TASKS			
View list of available scripts.	My Script, Shared Script	Scripts	
Create or upload and store a script.	My Script	Scripts	
Edit, delete, or view a stored script.	My Script	Scripts	
View version history of a stored script.	My Script	Scripts	

Table 6: Permissions Required for Script Tasks

SCRIPT TASK	SCRIPT TYPE	REQUIRED PERMISSIONS FOR SCRIPT TASK AND TYPE	COMMENTS
Create or upload and store a script.	Shared Script	Scripts Edit Shared Scripts	
Edit, delete, or view a stored script.	Shared Script	Scripts Edit Shared Scripts	
View version history of a stored script.	Shared Script	Scripts Edit Shared Scripts	
SCRIPT EXECUTION TASKS			
Execute a script (as root or local system).	Shared Script	Wizard: Run Scripts Read & Write (for servers associated with customers, facilities, or server groups)	A Shared Script always executes on a server as root or local system.
Execute a script (requires a password).	My Script	Wizard: Run Scripts Scripts Read & Write (for servers associated with customers, facilities, or server groups)	With *Wizard: Run Scripts* and *Scripts* permissions, execution of a My Script requires the use of a password.

Table 6: Permissions Required for Script Tasks

SCRIPT TASK	SCRIPT TYPE	REQUIRED PERMISSIONS FOR SCRIPT TASK AND TYPE	COMMENTS
Execute a script (as root or local system).	My Script	Wizard: Run Scripts Scripts Run My Script As Root Read & Write (for servers associated with customers, facilities, or server groups)	With *Run My Script As Root* permission, no password is required. Without this permission, the user can still execute the script, but only with a password.
Create (or upload) and then execute an *Ad-Hoc Script* (requires a password).	Ad-Hoc Script	Wizard: Run Scripts Scripts Read & Write (for servers associated with customers, facilities, or server groups)	With *Wizard: Run Scripts* and *Scripts* permissions, a password is required to execute an Ad-Hoc Script.
Create (or upload) and then execute an *Ad-Hoc Script* (as root/local system).	Ad-Hoc Script	Wizard: Run Scripts Scripts Run My Script As Root Read & Write (for servers associated with customers, facilities, or server groups)	With *Wizard: Run Scripts*, *Scripts*, and *Run My Script As Root* permissions, an Ad-Hoc Script executes on the servers as root/local system (without a password).

Table 6: Permissions Required for Script Tasks

SCRIPT TASK	SCRIPT TYPE	REQUIRED PERMISSIONS FOR SCRIPT TASK AND TYPE	COMMENTS
View execution results data.	My Script, Shared Script, Ad-Hoc Script	• Wizard: Run Scripts	The *Wizard: Run Scripts* permission allows a user to view results information for any executed script.

Predefined User Group Permissions

The following table lists the permissions of the predefined user groups for the features in the Opsware Command Center. An X in a table cell indicates that the group has permission to use the feature. The headings in the table columns abbreviate the names of the user groups as follows:

- **Basic**: Basic Users
- **Inter**: Intermediate Users
- **Adv**: Advanced Users
- **OSA**: Opsware System Administrators
- **Admin**: Administrators

Table 7: OCC Permissions of the Predefined User Groups

FEATURE NAME	BASIC	INTER	ADV	OSA	ADMIN
FEATURE TAB					
Configuration Tracking	X	X	X		
Configure Opsware				X	
Customers	X	X	X		X
DNS	X	X	X		
Data Center Intelligence Reports			X	X	

Table 7: OCC Permissions of the Predefined User Groups

FEATURE NAME	BASIC	INTER	ADV	OSA	ADMIN
Facilities	X	X	X		X
IP Ranges and Range Groups	X	X	X		
ISM Controls	X	X	X		
Manage Gateway				X	
Managed Servers and Groups	X	X	X	X	
Model: Applications	X	X	X		
Model: Hardware	X	X	X		
Model: Opsware			X		
Model: Service Levels	X	X	X		
Multimaster				X	
Operating Systems		X	X		
Packages	X	X	X		
Patches			X		
Scripts	X	X	X	X	
Server Attributes			X	X	
Server Pool		X	X		
System Diagnosis			X	X	
Templates	X	X	X		
Wizard: Custom Extension			X	X	
Wizard: Install Template	X	X	X		
Wizard: Install Patch	X	X	X		
Wizard: Install Software	X	X	X		
Wizard: Microsoft Patch Update	X	X	X		
Wizard: OS Provisioning	X	X	X		
Wizard: Prepare OS	X	X	X		
Wizard: Reconcile	X	X	X		

Table 7: OCC Permissions of the Predefined User Groups

FEATURE NAME	BASIC	INTER	ADV	OSA	ADMIN
Wizard: Run Scripts	X	X	X	X	
Wizard: Uninstall Patch	X	X	X		
Wizard: Uninstall Software	X	X	X		
Wizard: Upload Patch	X	X	X		
OTHER TAB					
Edit Shared Scripts			X	X	
Run My Scripts as Root	X	X	X	X	
Deactivate		X	X		
Allow Run Refresh Jobs					
Manage Public Server Groups				X	
Model Public Server Groups					
Locking: Application Servers		X	X		
Locking: Database Servers		X	X		
Locking: Other Applications		X	X		
Locking: OS Extras		X	X		
Locking: Service Levels		X	X		
Locking: System Utilities		X	X		
Locking: Web Servers		X	X		

Only the Administrator group also has permission to manage Opsware users and user groups, a feature not listed on the Opsware Command Center tabs.

All predefined groups have Read & Write permission to the categories listed in the Node Stacks tab of the Opsware Command Center. These categories include the subtrees of the software application tree, as well as service levels.

The following table lists the permissions of the predefined user groups for the OCC Client features. The table cells contain the following abbreviations:

- **R**: Read (only)
- **RW**: Read & Write

- **Y**: Yes
- **N**: No or None

Table -8: OCC Client Permissions of the Predefined USer Groups

FEATURE NAME	BASIC	INTER	ADV	OSA	ADMIN
APPLICATION CONFIGURATION					
Configuration	N	R	RW	N	N
Configuration Files	N	R	RW	N	N
Configuration on Servers	N	R	RW	N	N
Allow Check Consistency on Servers	N	N	Y	N	N
COMPLIANCE					
Audit Templates	N	R	RW	N	N
Audit Results	N	R	RW	N	N
Snapshot Templates	N	R	RW	N	N
Snapshots (specific to servers)	N	R	RW	N	N
Selection Criteria	N	R	RW	N	N
Allow General Snapshot Management	N	Y	Y	N	N
VISUAL PACKAGER					
Allow Create Package	N	N	Y	N	N
AGENT DEPLOYMENT					
Allow Deploy Agent	N	N	Y	N	N
Allow Scan Network	N	N	Y	N	N

Code Deployment User Groups

The following tables describe the capabilities of the Code Deployment user groups. For more information, see the Accessing Code Deployment & Rollback section of the *Opsware® SAS 5.2 User's Guide*.

Table 9: Special Code Deployment User Groups

CODE DEPLOYMENT USER GROUP	DESCRIPTION
Super User	Can define, request, or perform any code deployment operation on hosts designated for either staging or production. Because a Super User can perform operations on hosts associated with any customer, only a few users should belong to this group.
History Viewer	Can view a log of operations (service operations, synchronizations and sequences) that have been previously executed from the Code Deployment feature. Viewing this information can help you determine the status of particular deployment operations, and whether they completed successfully.

Table 10: Service User Groups

CODE DEPLOYMENT USER GROUP	DESCRIPTION
Service Editor	Can define a service, and modify or delete service definitions.
Production Service Performer	Can directly perform or request performance of service operations on hosts designated for use in production.
Staging Service Performer	Can directly perform or request performance of service operations on hosts designated for use in staging.
Production Service Requester	Can request performance of service operations on hosts designated for use in production.
Staging Service Requester	Can request performance of service operations on hosts designated for use in staging.

Table 11: Synchronization User Groups

CODE DEPLOYMENT USER GROUP	DESCRIPTION
Synchronization Editor	Can define a synchronization, and modify or delete the synchronization definition.
Synchronization Performer	Can directly perform or request performance of a synchronization action.
Synchronization Requester	Can request performance of a synchronization action.

Table 12: Sequence User Groups

CODE DEPLOYMENT USER GROUP	DESCRIPTION
Sequence Editor	Can define a sequence, and modify or delete the sequence definition.
Production Sequence Performer	Can directly perform or request performance of a sequence of actions on hosts designated for use in production.
Staging Sequence Performer	Can directly perform or request performance of a sequence of actions on hosts designated for use in staging.
Production Sequence Requester	Can request performance of a sequence of actions on hosts designated for use in production.
Staging Sequence Requester	Can request performance of a sequence of actions on hosts designated for use in staging.

Index