Opsware® System 5.1 Release Notes

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.

T + 1 408.745.1300 F +1 408.745.1383 www.opsware.com

Table of Contents

Introduction to Opsware System 5.1

The Opsware System 5.1 provides a new set of features, performance enhancements, and automation tools. This section provides a general description of these changes and provides references to more detailed explanations. The following new features are currently available:

- Express Automation Feature Set (referred to as the OCC Client in the Opsware System documentation)
- Server Group Enhancements
- Enhanced User Access and Authentication
- Access Control Boundaries for Server Groups
- Satellite Installation and Management
- Architecture Improvements
- Data Center Intelligence Reports
- Custom Fields
- ISM Controls
- Usability Enhancements
- SAS Content Pack 5.1
- DCML Exchange Tool (DET) Support for SAS Content Pack 5.1
- IDK Version 2.0 and WSAPI Version 2.1
- Context Sensitive Help for the OCC Client

All Opsware System features support cross-platform environments and are designed to automate both new and existing facilities.

What's New In Opsware System 5.1

Express Automation Feature Set

The Opsware System is made up of a set of features that automate IT processes. These features are designed to improve the speed, efficiency, and reliability of your systems and replace ad hoc, error-prone, manual processes. (See Chapter 3 in the *Opsware System 5.1 User's Guide* for more information.) These new features include:

- **Discovery and Agent Deployment**: The Opsware Discovery and Agent Deployment feature allows you to deploy Opsware Agents to a large number of servers, enabling you to remotely deploy the Opsware Agent to servers in your facility and place them under Opsware management. See Chapter 6 in the *Opsware System 5.1 User's Guide* for more information.
- **Server Explorer**: The Servers feature of the OCC Client allows you to browse and manage servers and server groups in your facility. Using the Server Explorer, you can perform an audit, take a snapshot, configure applications, view summary and history information, and browse the file system. You can also review registry information, hardware inventory, software lists, patch lists, services, properties, configurable applications, and even server history. See Chapter 5 in the *Opsware System 5.1 User's Guide* for more information.
- **Server Compliance**: The Opsware Server Compliance feature enables you to keep managed servers up-to-date and in compliance. The system compares servers to compliant working servers that perform as expected. If the managed servers differ from the compliant server, the system can detect it during an audit and you can install software and server objects to remediate the discrepancy. See Chapter 8 in the *Opsware System 5.1 User's Guide* for more information.

- **Visual Packager**: The Visual Packager 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. See Chapter 9 in the *Opsware System 5.1 User's Guide* for more information.
- **Application Configuration Management**: Opsware Application Configuration Management (ACM) enables you to create templates that help manage configuration files associated with applications. Using ACM, you can manage and update application configuration files from a central location. This ensures that applications in your facility are accurately and consistently configured. ACM also supports a rollback feature that creates a record of the application configuration before a change is made, and enables you to roll back to the original application configuration. See Chapter 15 in the *Opsware System 5.1 User's Guide* for more information.
- **Global Shell and Remote Terminal**: 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 the Opsware System. 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. See Chapter 10 in the *Opsware System 5.1 User's Guide* for more information.

Server Group Enhancements

With this release, any operation that you can perform on a single server you can now perform on groups of servers, and you can group servers in a variety of ways to meet your needs. See Chapter 7 in the *Opsware System 5.1 User's Guide* for more information.

- **Dynamic Groups**: These groups contain servers that are added to or removed from the group based on a set of user-defined rules. If the rules are changed or the servers in the environment change, servers will be added to or removed from the group automatically. Rules apply only to the group being created or modified, not to any subgroups.
- **Private Groups**: If you belong to a user group that has access to the Manage Servers list, you can create groups that you alone can see and work with. Only you see your private groups – other Opsware users cannot see them. Private groups behave the same way as public groups, with the exception that modeling is not available for private groups.
- **Ability to Run Operations on Groups**: The Server Groups feature is useful for gathering servers into collections. These groups can be used as a shortcut for performing the same action on all of the servers simultaneously, instead of performing the action on each individual server, one at a time. Server groups can also be used to simply organize groups of servers.
- **Ability to Filter the Manage Server List by Types of Groups**: You can modify your views of servers and server groups by selecting Summary, Hardware, Software, and Communications from the View menu. You can also elect to further modify your view by selecting Servers and Groups, Servers Only, or Groups Only.
- **Search**: You can locate, list, and display servers in the Opsware Command Center by searching with the name, hostname, or IP address. You can also view the Manage Servers list and Server Pool list when you want to see a complete list of all your servers. You can refine the lists by using filters, and

you can browse nodes in the Software Tree by viewing servers sorted by hardware category.

User Authentication

This new authentication mechanism stores information in the Model Repository, eliminating the need for separate authentication and access directory. It also supports LDAP servers.

Additionally, the new authentication mechanism supports setting permissions for the new OCC Client features. The Client Features tab allows you to set permissions for new OCC Client features.

See Chapter 3 in the *Opsware System 5.1 Configuration Guide* for more information.

Access Control Boundaries for Server Groups

On the Edit Groups page of the Opsware Command Center, there are new tabs for Server Groups. The Server Groups tab enables you to control access to managed servers according to their membership in the public server groups.

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.

Opsware Satellite

This release provides Opsware Satellite Installation, and a user interface for managing Opsware Gateways. This Satellite system enables you to manage servers with duplicate IP addresses in remote facilities and limit the network traffic between Opsware Cores or Satellites. See Chapter 3 in the *Opsware System 5.1 Administration Guide* for more information.

Multimaster Traffic over the Gateway

In Opsware System 5.1, multimaster traffic between Opsware Cores in a multimaster mesh is sent through the Opsware Gateway. The Opsware System is configured automatically to send multimaster traffic through the Opsware Gateway when you install and configure a multimaster mesh.

See Chapter 6 in the *Opsware System 5.1 Deployment and Installation Guide* for more information.

Manage Gateway User Interface for Satellites and Cores

The Manage Gateway feature enables you to obtain debugging and status information about the gateways and the tunnels between gateways. It also enables you to perform specific tasks for gateways, such as changing the bandwidth limits, changing the tunnel cost between gateway instances, restarting gateway processes, or changing the logging levels for gateway processes.

To access the Manage Gateway feature, you must have the Manage Gateway permission (Users & Groups > Edit Group > Features tab) in the Opsware System. By default, this permission is included in the Opsware System Administrators group.

See Chapter 3 in the *Opsware System 5.1 Administration Guide* for more information about managing gateways.

See the *Opsware System 5.1 Configuration Guide* for information about user groups and Opsware permissions.

Satellite Installation through the Opsware Installer

The Opsware System 5.1 supports a new type of installation via an Opsware Satellite. With an Opsware Satellite, a full Opsware core is not installed in the facility. Instead, an Opsware Gateway and Software Repository Cache are installed. An Opsware Gateway provides network connection and bandwidth management to the satellite. The satellite must be linked to at least one core, which may be either standalone or multimaster. Multiple satellites can also be linked to a single core. See Chapter 7 in the *Opsware System 5.1 Deployment and Installation Guide* for more information.

Architecture Improvements

The system architecture in the Opsware System 5.1 has changed to support new features in the following ways:

- The Opsware Global File System (OGFS) Server has been added to the architecture. The OGFS Server dynamically constructs the Opsware Global File System (OGFS), a virtual file system. The Global File System Server component is installed on a Linux server in an Opsware core. The Global File System Server can connect to an Opsware Agent to open a Unix shell or a Windows Remote Desktop connection on a managed server.
- The functionality of the Opsware Gateway has been enhanced. In the Opsware System 5.1, The Opsware Gateway provides connectivity and network bandwidth management between Opsware cores in a multimaster mesh, between cores and Satellites, and between managed servers (Opsware Agents) and cores.
- The Opsware Access & Authentication Directory has been replaced in the Opsware System 5.1. In this release, the new authentication mechanism stores information in the Model Repository, eliminating the need for a separate authentication and access directory.

Data Center Intelligence Reports (DCI Reports)

DCI Reports provide real-time comprehensive information about an organization's servers, software, customers, operating systems, patches, compliance policies, and changes that have occurred and should occur. There are five reporting types available from the OCC navigation panel, each reporting area links to a set of related reports organized into folders. The following categories of reports have been improved or introduced with this release:

- **Server Reports**: These reports show server changes, facilities and customers, software and patches, and users and security for the Opsware Server Automation System (SAS).
- **Network Reports**: These reports display the network environment, status, and health, if the Opsware Network Automation System (NAS) has been installed.
- **Compliance Reports**: These reports help you comply with auditing standards, including COBIT, COSO, ITIL, and Sarbanes Oxley.
- **Custom Reports**: These are specific reports created for particular needs in your operational environment.
- **Ad-hoc Reports**: These reports enable you to create reports about specific software, servers, patches, and the Opsware model, and enable you to group and filter them according to your needs.

See the *Opsware System Data Center Intelligence 1.5 Administrator's Guide* for more information.

Custom Fields

In the Opsware System, you can store custom server data that is specific to your operational environment in custom fields. Using these fields, you can add files, URLs, text strings, numbers, and dates, and search for servers based on a stored value. Also, you can use a custom field as criteria to create a dynamic server group. See Chapter 7 in the *Opsware System 5.1 User's Guide* for more information.

ISM Controls in the OCC

An Intelligent Software Module (ISM) is an installable software package created with the Opsware ISM Development Kit (IDK). An ISM can contain control scripts, installation scripts, and un-installation scripts. These scripts enable you to more efficiently manage applications and package installation. See the *Intelligent Software Module (ISM) Development Kit 2.0 Guide* for more information about building and uploading ISMs into the Opsware System.

With this release, you can now run control scripts from the Control window of the Opsware Command Center and perform day-to-day, application-specific tasks such as starting software servers.. See Chapter 11 in the *Opsware System 5.1 User's Guide* for more information about using ISM Controls.

Usability Enhancements throughout Opsware Command Center

The usability of the Opsware Command Center UI has been enhanced in the following ways:

- Opsware Command Center wizards have been streamlined. The Overview page has been removed and the Preview page is now optional. Additionally, you can select individual servers and server groups in any wizard. When running a wizard on a server group and scheduling the job, you can specify to refresh the group before the job runs.
- All icons in the Opsware Command Center UI have been redesigned to include new Opsware System 5.1 features and to clearly distinguish their functions.
- The left and top navigation panels in the UI have been reorganized to include new features.
- The Manage Server list has been enhanced by restructuring the commands in the menu bar, reorganizing the tabs to include server groups, allowing you to edit which filters to display, and providing the ability to change the number of servers that display per page.
- Installation of software from the Applications feature (the Software Tree) is enabled by the addition of an Install Button in each Software Tree node.
- Installation and uninstallation of patches from the Patches list is enabled by the addition of Install and Uninstall Buttons in the View Patch page for each patch.

- The Manage Packages feature is enhanced to support adding packages to nodes from the Packages list. Additionally, this feature contains a link to download each package from the package's properties page.
- Navigation in the Applications feature (the Software Tree) has been enhanced by the addition of a Folder Up icon to move up the node hierarchy and by the relocation of the buttons in the node view to indicate the button functions in the Software Tree.
- In the Operating Systems list, the UI includes a link (Install OS) for each OS displayed in the list. (In previous releases, you had to select the checkbox for an OS, and then click the Install OS button to launch the Install OS Wizard.)

SAS Content Pack 5.1

The SAS Content Pack 5.1 provides an additional set of templates, scripts, and audit compliance selection criteria that enable you to more efficiently manage your content. See Appendix A in the *Opsware System 5.1 User's Guide* for more information.

The Contact Pack includes:

- **Application Configurations**: Application configurations are designed to help you manage typical configuration files associated with applications or operating systems. Using ACM inside the OCC Client enables you to edit values in a configuration file and push those changes to the application on managed servers. The ACM templates provided in this release are system templates that manage operating system configuration files, service templates that manage service configuration files, and application templates that manage application configuration files.
- **Global Shell Scripts**: Global Shell scripts run on managed servers that have the following operating systems: AIX, HP-UX, Linux, Solaris, and Windows. These scripts are executed on servers that are in the Opsware Global File System (OGFS).
- **Snapshot Selection Criteria**: Snapshot selection criteria specify the information you want to capture about the state and configuration of a

managed server or server group, at a particular point in time. A snapshot template identifies this selection criteria. Since selection criteria are specific to an operating system, such as Unix, Linux, or Windows, you cannot have one (universal) snapshot template for different operating systems of managed servers in your Opsware System.

DCML Exchange Tool 2.0 (DET 2.0)

DET 2.0 now supports importing and exporting Application Configuration and Compliance Criteria content.

ISM Development Kit Version 2.0 (IDK V2.0)

The IDK V2.0 has several new features that enable you to more efficiently apply scripts. They include:

- **Shared Runtime Packages**: If you upload multiple ISMs into a core, just one copy of the runtime package is stored in the Software Repository. Likewise, if you install multiple ISMs onto a managed server, just one copy of the runtime package is installed.
- **Passthru Packages**: You can associate third-party packages with an ISM. The IDK copies these passthru packages to the ISM's package subdirectory, does not unpack them, and uploads them unchanged.
- **Metadata Update**: You can specify the metadata properties of packages and software nodes with the IDK before uploading the ISM.

See the *Intelligent Software Module (ISM) Development Kit 2.0 Guide* for more information.

Web Services API Version 2.1 (WS API V2.1)

The Opsware System provides SOAP-based application programming interfaces that allow users to perform specific operations on database fields. In this release, WS API clients can catch specific OpswareExceptions, instead of generic RemoteExceptions.

For the SOAP layer, JBoss instead of WebLogic will be used for the server side of the WS API. This change should not affect the client view of the API. See the *Opsware System Web Services API 2.1 Guide* for more information.

Context Sensitive Help for the OCC Client

Opsware Online Help describes how to use the Opsware System 5.1, starting with an introduction to the system and how to navigate the user interface. It provides information about managing servers, operating system provisioning, managing software packages, provisioning applications, managing patches, reconciling servers, and deploying and rolling back code. It also reviews automated script execution and automated configuration tracking. In addition, Context Sensitive Help is provided for the Opsware Command Center Client. The Online Help System contains the Opsware System User's Guide, the Administrator's Guide, and a glossary.

Platform and Environmental Support

Supported Operating Systems, Package Types, and File Types

The following table shows the operating systems, package types, and file types that Opsware System 5.1 supports. For complete information on package types and file types, see Chapter 5, Package Management, in the *Opsware System 5.1 User's Guide*.

Operating System and Version	Package Type	File Types
SPARC-processor-based hardware (sun4u, sun4us)		
SunOS (5.6, 5.7, 5.8, 5.9), Beta support for the Solaris 10 Early Access Release	Solaris Package	uncompressed datastream
	Solaris Patch	.zip, .tar, .tar.Z, .tar.gz, .tgz, .jar
	Solaris Patch Cluster	.zip, .tar, .tar.Z, .tar.gz, .tgz
	RPM	.rpm
x-86-processor-based hardware		
Red Hat Linux (6.2, 7.1, 7.2, 7.3, 8.0, Advanced Server 2.1, Advanced Server 3.0, Enterprise Server 2.1, Workstation 2.1,Enterprise Server 3.0, Workstation 3.0)	RPM	.rpm
SUSE Linux (Enterprise Server 8.0, Standard Server 8.0, Enterprise Server 9.0)	RPM	.rpm
Microsoft Windows (NT 4.0, Windows 2000 Server Family, Windows Server 2003)	Hotfix	.exe
	Service Pack	.exe

Operating System and Version	Package Type	File Types
	MSI	.msi
	ZIP	.zip
	Security Patch	.exe
	Windows Utility	.exe
	Microsoft Patch Database	.xml, .cab
IBM-POWER-processor-based hardware		
IBM AIX (4.3, 5.1, 5.2, 5.3)	RPM	.rpm
	LPP	.bff
	Base Fileset	N/A
	Update Fileset	N/A
	APAR	N/A
	Maintenance Level	N/A
HP PA-RISC-processor-based hardware		
HP-UX (10.20, 11.00, 11.11/11i v1)	Depot	.tar
	Product	N/A
	Fileset	N/A
	Patch Product	N/A
	Patch File	N/A

***Note**: Patch files for HP-UX 10.20 are packaged like other software files, and are not specified as patch file types. Consequently, you cannot install patches for HP-UX with the Patch Wizard; you can only install them with the Install Software Wizard.*

Supported Browsers

The Opsware System 5.1 supports the following browsers:

Browser	Windows 2000	Windows 2003	Windows XP	Linux	Solaris	Apple OS
Microsoft Internet Explorer 5.5	X					
Microsoft Internet Explorer 6.0	X	X	X			
Firefox 1.0	X	X	X	X	X	X
Mozilla 1.6	X	X	X	X	X	X

Supported Core Operating Systems

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

Supported Operating System for Opsware core	Versions
Sun Solaris	Solaris 8 Solaris 9
Red Hat Linux	Red Hat Enterprise Linux 3AS

The following table lists the supported operating systems for the Opsware Satellite.

Supported Operating System for Opsware Satellite	Versions
Sun Solaris	Solaris 8 Solaris 9
Red Hat Linux	Red Hat Enterprise Linux 2.1AS Red Hat Enterprise Linux 3AS

The Data Center Intelligence Server runs on Windows 2000 and 2003.

Supported Installations

The Opsware System 5.1 release supports the following installations:

- First time, from-scratch installation of a stand-alone core
- First time, from-scratch installation of multimaster cores
- First time, from-scratch installation of Satellite

Documentation

This release comes with the following documentation:

- *Opsware System 5.1 Release Notes*
- *Opsware System 5.1 Deployment and Installation Guide*
- *Opsware System 5.1 User's Guide*
- *Opsware System 5.1 Configuration Guide*
- *Opsware System 5.1 Administration Guide*
- *Opsware System 5.1 Planning Guide*
- *Opsware System 1.5 Data Center Intelligence Administrator's Guide*
- *Opsware System DCI 1.5 Release Notes*
- *DCML Exchange Tool 2.0 Reference Guide*
- *OCLI 2.0 Reference Guide*

The Opsware System documentation is available online at
https://download.opsware.com/documentation/

Ask your Opsware administrator for the user name and password to access the site.

The following documentation will be available in the download site:

- *Opsware System Web Services API 2.0 Guide*
- *Opsware System Intelligent Software Module (ISM) Development Kit 2.0 Guide*
- *CML Tutorial for Opsware System 5.1*

What's Fixed in Opsware System 5.1

The following bugs have a severity level of Critical or Major and are fixed in Opsware System 5.1.

Bug ID: 10969

Description: In the Manage Server List, a 500 error appears when displaying server properties for a server that is attached to a customer that was added without refreshing the Manage Customers page.

Subsystem: Opsware Command Center > Customers feature

Platform: Independent

Resolution: Fixed.

Bug ID: 13441

Description: Customer lists in the Opsware Command Center and the Opsware Access & Authentication Directory could get out of synch when the command `ldapmodify` was used to add an Opsware customer directly to the Opsware Access & Authentication Directory.

Subsystem: Opsware Command Center > Customers feature

Platform: Independent

Resolution: Fixed. In Opsware System 5.1, user access and authentication no longer uses the Access & Authentication Directory because user access and authentication data are stored in the Opsware Model Repository.

Bug ID: 14864

Description: The Opsware System has a device selection limit for operations. The maximum number of devices that can be selected and acted on varies, but is usually between 60 and 70. Selecting too many servers to act on can display a JavaScript error.

Platform: Independent

Subsystem: Opsware Command Center > Manage Servers

Resolution: Fixed. In Opsware System 5.1, the Manage Server page allows you to specify the number of servers to display per page.

Bug ID: 15680

Description: If the Oracle database ran out of table space, the Opsware Model Repository Multimaster Component failed to apply the Opsware multimaster transaction that caused Oracle to run out of table space. The failure could cause cascading Opsware multimaster conflicts even after the table space problems got resolved.

Subsystem: Model Repository Multimaster Component

Platform: Independent

Resolution: Fixed. The Opsware System checks the Oracle error string and only generates a multimaster conflict when the error string matches an Oracle error that could throw conflicts, such as Oracle foreign and unique key constraint errors, check constraint errors, NOT NULL constraint errors, and so on. The Opsware System also generates a multimaster conflict when it receives a non-Oracle error. In the majority of cases, this is a Conflicting Data error.

Bug ID: 15722

Description: Components will start and appear to be up, but will not properly authenticate anyone who attempts to log in to them. Core components appear to field connections before the components they depend on are up. The Command Engine attempts to contact the Data Access Engine in order to determine configuration parameters, including what authentication domain should be used for the Access & Authentication Directory. When the Data Access Engine cannot be contacted, it reverts to using loudcloud.com as the authentication domain.

Subsystem: Data Access Engine

Platform: Independent

Resolution: Fixed. In Opsware System 5.1, the component configuration files used by the Opsware Installer were extended to include a %verify_pre and %verify_post sections. The %verify_pre section lists a set of conditions that must be true before

installing a component. The %verify_post section lists a set of conditions that must be true after the component has been installed. If any one of the conditions in %verify_pre or %verify_post fails, the invocation of the installer will return a non-zero exit status (indicates failure).

Bug ID: 16105

Description: Opsware managed servers were required to resolve unqualified names. Windows servers that use DNS but do not have a DNS search order set for them (they could only resolve fully qualified names) could not communicate with an Opsware core.

Subsystem: Opsware Command Center > Manage Servers

Platform: Independent

Resolution: Fixed. In Opsware System 5.1, the Opsware Agent does not perform DNS lookups. When an Opsware Agent is installed on a server, the Opsware Agent is given an IP address to find the Opsware Gateway. The Opsware Gateway mediates all communication between the Opsware Agent on the server and the Opsware core. The Opsware Agent no longer requires DNS to resolve any domain names.

Bug ID: 17801

Description: A race condition could occur during Opsware installation on a slow machine. The Opsware Agent installed on a core server could attempt to register with the Opsware core when the Data Access Engine had not started.

Platform: Linux, Solaris

Subsystem: Opsware Installer

Resolution: Fixed. In Opsware System 5.1, the Opsware Agent configuration file (agent.conf) includes a check for Data Access Engine availability in the %verify_pre section of the file.

Bug ID: 17854

Description: The Opsware Installer fails when the Command Engine is installed on a server by itself and the other Opsware components are not installed yet. The

Command Engine fails to start and the Opsware Installer fails because the file `pyiconv.conf` is missing symbolic links:

```
%post
/lc/bin/lcdepot
```

Subsystem: Opsware Installer

Platform: Independent

Resolution: Fixed.

Bug ID: 18386

Description: The Opsware Build Manager component occasionally stops outputting logs to the directory `/var/lc/buildmgr/servers/`. No new logs are created or appended to the `/servers/` directory.

Subsystem: OS Provisioning

Platform: Independent

Resolution: Fixed.

Bug ID: 21096

Description: Sorting behavior in the Opsware Command Center behaved in the following way.

All column lists of items presented in the UI sort in the following order:

- All items from A-Z
- All items from a-z

Expected behavior is for listed items to sort according to this order:

- All items from Aa-Zz

In some cases, items were not being sorted at all.

Platform: Independent

Subsystem: Opsware Command Center User Interface

Resolution: Fixed. Added the `NLS_SORT=punctuation` setting directly in the file `setEnv.sh` and in the file that is generated from the Opsware Installer component configuration file `twist.conf`.

Bug ID: 21254

Description: The Opsware System performs many redundant LDAP searches for the admin user, which affects the performance of the Opsware Command Center.

Subsystem: Opsware Command Center

Platform: Independent

Resolution: Fixed. In Opsware System 5.1, user access and authentication no longer uses the Access & Authentication Directory (which relies on an LDAP server) because access and authentication data is stored in the Opsware Model Repository.

Bug ID: 21264

Description: The Model Repository (truth) export fails when exporting large amounts of data from the database. The Oracle dump completes successfully, but gzip is compiled with `stat` instead of `stat64` and the export fails while attempting to gzip the file.

Subsystem: Model Repository

Platform: Independent

Resolution: Fixed. The export involved several stages and used temporary files in two locations—one in the `/tmp` directory. In Opsware System 5.1, the Opsware Installer uses a single pipeline to create the gzipped tarball with the dumps and uses a single pipeline to extract them when importing the data into a Model Repository. The Opsware Installer cats the export file and pipes it into `gzip -d`. In Opsware System 5.1, the export file is named `truth_data.tar.gz` instead of `truth_data.tar`.

Bug ID: 21459

Description: Installing an ISM on a server fails when the installation retrieves a custom attribute value from the ISM that has non-ASCII characters, for example: # ÃÊ±âÈÇÏ´Â Áß...

Subsystem: ISMs and Software Provisioning

Platform: Independent

Resolution: Fixed in the Opsware ISM Development Kit v1.0.5.

Bug ID: 21519

Description: The Reschedule screen in My Jobs displays a vague message and the Save button becomes unavailable if you select the original time for the job to run. The message indicates the range of time and not the exact time during which you cannot reschedule the job.

Subsystem: Opsware Command Center > My Jobs

Platform: Independent

Resolution: Fixed.

Bug ID: 21576

Description: The Model Repository Multimaster Component (vault) needed the latest JDBC driver.

Subsystem: Model Repository Multimaster Component

Platform: Independent

Resolution: Fixed. The latest JDBC drivers that ship with Oracle 9.2.0.4.0 have been added to the Opsware Installer distribution for Opsware System 5.1.

Bug ID: 21672

Description: The configuration script for DCI, `configDCI` contains several errors:

- On the first line, there is a space between `#!` and `/bin/sh`
- `mv` is hardcoded as `/usr/bin/mv` (`mv` is `/bin/mv` in Linux)
- `authproxy.destVIP` is hardcoded as `occ.opsware.com`

Subsystem: Data Center Intelligence Reporting

Platform: Independent

Resolution: Fixed. The script issues are resolved and the correct configuration has been incorporated in the Opsware DCI v1.5, which ships with Opsware System 5.1.

Bug ID: 21708

Description: Because of the MBSA upgrade check, software registration and reconcile for Windows servers is slow when the Opsware System must connect to the Internet through a firewall. On every invocation, the program mbsacli.exe tries to

contact Microsoft.com to check for updates. During software registration, the Opsware System invokes mbsacli.exe multiple times, which can cause a delay of up to three minutes.

Subsystem: Opsware Command Center > Software Provisioning

Platform: Windows

Resolution: Fixed. In Opsware System 5.1, mbsacli.exe is invoked with the -nvc option so that it bypasses the new version check.

Bug ID: 21899

Description: When installing a subsequent Opsware core in a multimaster mesh, the Opsware Installer allows the installation to proceed when the crypto database from the primary core is not imported into the core being installed. Consequently, the core being installed incorrectly resigns all the Command Engine scripts and the primary core exhibits unpredictable behavior.

Subsystem: Opsware Installer

Platform: Independent

Resolution: Fixed. When installing an Opsware core, the Opsware Installer lists the Opsware Certification Tool as a prerequisite for the Model Repository component. You are required to generate new crypto or copy previously generated crypto from the primary core. Additionally, all Opsware components that depend on the crypto database include a prerequisite check to verify the existence of the following file:
/var/lc/crypto/cadb/realm/opsware-crypto.db.e
If this file doesn't exist, the install terminates.

Bug ID: 21905

Description: When running the Software Install Wizard or Software Uninstall Wizard on large numbers of servers, the wizard could stop responding and, during the Preview Reconcile step, the Next button would stay disabled. The wizard then had to be restarted from step 1.

Subsystem: Opsware Command Center > Install Software Wizard and Uninstall Software Wizard

Platform: Independent

Resolution: Fixed. In Opsware System 5.1, users can skip the Preview Reconcile step in the wizards and proceed directly to installation or uninstallation. Additionally, the wizard behavior was changed so that it finishes reloading the server list before refreshing the page.

Bug ID: 21909

Description: During OS provisioning, if a template containing a Service Level is used, the Service Level/Agent node is not attached to the server. This leads to the following data integrity error:

```
Opsware Services (Finds any problems with server
attachments to the Opsware Services nodes.): Server IDs
with no Agent attachment: [52240105]
```

Platform: Platform Independent

Subsystem: Data Access Engine

Resolution: Fixed. In Opsware System 5.1, servers are attached to or below correct Opsware Agent node.

Bug ID: 21933

Description: Re-provisioning an Opsware managed server with Solaris 10 sets the server to single user mode. When re-provisioning the OS on a server with Solaris 10 Early Access Release (beta support), the server is set to System Maintenance Mode (also known as single user mode) and a prompt appears allowing you to override the system's default NFS version 4 domain name.

Subsystem: OS Provisioning

Platform: Solaris 10

Resolution: Fixed. Opsware System 5.1 includes a custom attribute to allow you to set the NFSv4 default domain in the Opsware Command Center. The custom attribute corresponds to the equivalent keywords in the `sysidcfg` file.

KEYWORD	DESCRIPTION
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.

Bug ID: 21965

Description: In the Prepare OS wizard, the valid characters allowed for the name of the operating system are A-Z, a-z, 0-9,_.-,@,( ),[space]. But stricter rules are enforced for the name of the operating system in the Edit Operating System Page. (To access this page, click the Operating Systems link from the navigation panel on the Opsware Command Center Home Page. Select the name of the operating system you want to edit.) In the Edit Operating System page, the valid characters allowed for the name of the operating system are A-z, 0-9, _, -.

When you edit the properties for an OS definition, you will receive an error message when the OS definition name contains a-z, or @,( ),[space] characters.

Platform: Independent

Subsystem: Operating Systems

Resolution: Fixed. The Opsware Command Center allows you to enter lower-case letters when editing OS profile names.

Bug ID: 22326

Description: When patching or installing software on servers located in an Opsware Satellite, the Opsware Gateway stops responding and subsequently fails due to asynchronous SSL failures. The Data Access Engine is unable to communicate with the gateway's admin port listener. The Data Access Engine connects to the gateway's

admin port once a minute to retrieve the health and status of all connected Satellites. This connection uses an asynchronous SSL client library.

Subsystem: Opsware Gateway

Platform: Independent

Resolution: Fixed. The timeout that the Data Access Engine uses to contact the Opsware Gateway admin port was increased from five seconds to ***XX*** seconds. Additionally, when a timeout occurs, the Data Access Engine shuts down the open sockets for the gateway. The Opsware Gateway's admin port uses a non-blocking socket when the *SSL_accept*() routine cannot continue the handshake.

Bug ID: 22757

Description: The custom attributes values set for a server are not overriding the values of those custom attributes set for an OS profile. For example, if the PARTITION_SIZE custom attribute is set for an OS profile and a server. The server uses the value set for the OS profile.

OS -> PARTITION_SIZE = 1000

Device -> PARTITION_SIZE = 2000

The 'getCustomAttr("PARTITION_SIZE")' returns '1000'.

Subsystem: Opsware Command Center > Manage Servers

Platform: Independent

Resolution: Fixed. The custom attribute values set for servers override the values set for OS profiles.

Bug ID: 23084

Description: The Install OS Wizard stops responding when it has to display a large number of templates in step 4 (Select Template) of the wizard and a Standard 3100 error is displayed in the page.

Subsystem: Opsware Command Center > Install OS Wizard

Platform: Independent

Resolution: Fixed. The query that the Opsware System uses to display the OS templates is more efficient and the page displays the results in a few seconds.

Bug ID: 24019

Description: Running an ad-hoc script on a server does not add an entry for the operation to the server's history.

Subsystem: Opsware Command Center > Distributed Script Execution

Platform: Independent

Resolution: Fixed.

Bug ID: 25200

Description: When the ISM Development Kit (IDK) generates an error while uploading an ISM, sometimes it outputs a traceback to stdout or stderr and the traceback contains the password of the user who uploaded the ISM.

Subsystem: ISM Development Kit

Platform: Independent

Resolution: Fixed in the Opsware ISM Development Kit v2.0.3.

Bug ID: 25812

Description: If the package SUNWzlib is not installed on the server running the Web Services Data Access Engine, the Prepare OS Wizard fails and displays a traceback when creating a Linux OS profile.

Subsystem: OS Provisioning feature

Platform: Linux

Resolution: Fixed. The Opsware Installer verifies that the SUNWzlib package is installed on the server you are installing the Web Services Data Access Engine on.

Bug ID: 25922

Description: If a Conflicted Elsewhere message from a destination core to the source core is delayed, the multimaster conflict might get resolved before the message is received. When this happens, the Model Repository Multimaster Component (vault) re-locks all objects in the transaction. The Multimaster Tool finds conflicts by looking at the destination core only; therefore, these transactions do not reappear in the Multimaster Tools pages and you cannot unlock the objects.

Subsystem: Administration > Multimaster Tools

Platform: Independent

Resolution: Fixed. In the Multimaster Tools page, the MM State and Conflict Report data include invisible conflicts — conflicts that are marked conflicted_elsewhere but do not have any conflicts.

Known Problems, Restrictions, and Workarounds in Opsware System 5.1

Users should be aware of the following known problems in Opsware System 5.1.

Access and Authentication

Bug ID: 23457

Description: Changes to permissions are not reflected in the current session of the Opsware Command Center Client.

Platform: Platform Independent

Subsystem: Access and Authentication

Symptom: As an Opsware administrator, when you make changes to permissions in a user group, the changes are not propagated to the Server Explorer if a server browser is currently open in the Opsware Command Center Client.

Workaround: Close the server browser and open a new server browser.

Bug ID: 27675

Description: For delegated authentication, client certificates are not supported.

Platform: Platform Independent

Subsystem: Access and Authentication

Symptom: If the external LDAP server is configured to require client certificates, then the Opsware system is unable to successfully communicate with the external LDAP server. Specifying client certification properties in the twist.conf file does not help, because the external LDAP server expects a distinct client certificate per user.

Workaround: When connecting to an external LDAP server, use either of the following approaches:

- Simple bind over cleartext.
- Simple bind over anonymous SSL (no client certificate).

Bug ID: 27445

Description: The addition of an Application or Service Level node to Patch Install Order Tab fails with access denied error.

Platform: Platform Independent

Subsystem: Access and Authentication

Symptom: When you try to add an Application or Service Level node to Patch Install Order Tab, the operation fails with the following error:

```
Error ID:   16640444
Error Name:       Twist Method Error
Exception Info:   com.opsware.exception.TwistException
<message=''> <message=' <Access denied>
```

Workaround: To add an Application node to Patch Install Tab, you need the following permission:

Permission	Description
Model: Applications	Manage Application Nodes

To add a Service Level node to Patch Install Tab, you need the following permission:

Permission	Description
Model: Service Levels	Manage Service Level Nodes

To obtain the required permissions, contact your Opsware administrator.

Bug ID: 27800

Description: Creating a user group with the strings CDR, CDS, or CDT fails with an error.

Platform: Platform Independent

Subsystem: Users and Groups

Symptom: When you create a user group, with the string CDR, or CDS, or CDT in the group name, the newly created group will not be in the group list, and when you try to create the same group again, the operation fails with the following error.

```
The Group Name which you are trying to create is already
in use. Please enter another name and try again.
```

Workaround: While creating a new user group do not include the substring CDR, CDS, or CDT in the group name.

Code Deployment

Bug ID: 27529

Description: Run sequence fails if the user is not assigned to the CDS History Viewer group.

Platform: Platform Independent

Subsystem: Code Deployment

Symptom: When a user belonging to the CDS Production Sequence Performer group attempts to run a sequence, the sequence fails leading to the following error:

```
The input you entered was invalid or you tried to access
a resource not available to you. Please check the URL
entered or click the back button and check your input.
```

Workaround: In order to successfully run a sequence the user must be assigned to the CDS History Viewer group.

Configuration Tracking

Bug ID: 22674

Description: Adding a Configuration Tracking Policy entry to a server with an existing entry leads to an error.

Platform: Platform Independent

Subsystem: Configuration Tracking

Symptom: When you try to add a Configuration Tracking Policy entry to a server, which already has an existing entry, you get the following error:

```
OpswareError: spin.usage [ module: spinobj.py, method:
setBPD, line: 18749, hostname: m131.dev.opsware.com,
timestamp: 03/Mar/2005 230818, msg: Cannot overwrite
existing backup policy directive /etc/hosts:FILE ]
```

Workaround: Locate the server which already has the backup policy you are trying to set. Remove that backup policy from the server and try the operation again.

Content

Bug ID: 28117

Description: Application Configurations will not restart services not already running.

Platform: Unix/Linux

Subsystem: Content – Application Configuration

Symptom: At this time, application configurations will not start services that are not already running. In the event you wish to configure a Unix or Linux service that is not already running on a system, please start the service before using application configurations or you may get an error from the application configuration post-script execution. This error can be ignored, as the configuration has in fact been pushed to the server, but the service has not been started.

Workaround: Please start the service before using application configurations or you may get an error from the application configuration post-script execution.

DCML Exchange Tool

Bug ID: 25383

Description: Importing a template containing a Service Level or Application node with a special character ”/” in its name field results in the Service Level or Application node not being attached to the template.

Platform: Platform Independent

Subsystem: DET

Symptom: If you Import a template containing a Service Level or Application node with a special character ”/” in its name field, the template is imported but the Service Level or Application node is not attached to the template.

Workaround: None. Do not create a Service Level or Application node with special character ”/” in its name field.

Bug ID: 27940

Description: Special characters in Custom Attribute Value in XML export document causes error.

Platform: Platform Independent

Subsystem: DET

Symptom: Importing an XML export document containing any object strings that resemble XML tags (for example, </string>) in a Custom Attribute value leads to the following error:

```
Command Error Message: rethrew: {E301} XML document
structures must start and end within the same entity.
[root@copper1 joe]#
```

Workaround: When Importing an XML export document, do not use special characters containing any object strings that resemble XML tags (for example, </string>) in a Custom Attribute value.

Installer

Bug ID: 27268

Description: Linux portmapper can assign Opsware ports to Network File System (NFS) services.

Platform: Linux

Subsystem: Installer

Symptom: In Linux, the portmapper can assign Opsware ports to Network File System (NFS) service which can cause the installation of Opsware System to fail since the ports are not available.

Workaround: During installation add an entry for the component name and the port in the `/etc/services` file to prevent the portmapper from assigning Opsware ports to Network File System (NFS) services.

Operating System Provisioning

Bug ID: 26125

Description:

Platform: Platform Independent

Subsystem: OS Provisioning

Symptom: When you reprovision a server, the Opsware Command Center (OCC) uses the display name when displaying a server, whereas the Opsware Command Center Client (OCC Client) uses the hostname when displaying a server.
By default, when you first install an OS on a server, the Opsware Command Center populates the display name field with the hostname of the server. If a user resets this name after OS installation or when reprovisioning the server with a new OS, the name displayed in the Opsware Command Center and the name displayed in the OCC Client will not match.

Workaround: None

Opsware Agent

Bug ID: 26747

Description: The Agent Installer fails to create the registry key on a Win2K server if MS AntiSpyware is installed on the server.

Platform: Windows

Subsystem: Agent

Symptom: When you install an Opsware Agent on a Win2K server, the Agent Installer fails to create the registry key if MS AntiSpyware is installed on the server. As a result, the Opsware Agent is not installed successfully.

Workaround: In order to install an Opsware Agent successfully on a Win2K server with MS AntiSpyware, disable the MS AntiSpyware before installing the Opsware Agent.

Bug ID: 27360

Description: The Windows Agent Uninstaller prompts the user to restart the Windows server even though ogshcap.dll is not in use.

Platform: Windows

Subsystem: Agent

Symptom: During Opsware Agent uninstallation on a Windows server, the Agent Uninstaller will prompt the user to restart the server, if the ogshcap.dll is not in use and has been successfully deleted.

Workaround: Select the do not restart the server option and close the dialog box.

Bug ID: 27590

Description: Unable to access the C drive on Windows NT4 TSE server after installing an Opsware Agent.

Platform: Windows NT

Subsystem: Agent

Symptom: After installing an Opsware Agent on Windows NT4 TSE server, the C drive is not accessible via the Opsware Global Shell.

Workaround: None.

Opsware Command Center

Bug ID: 22865

Description: Uploading a large file in a custom field results in an error.

Platform: Platform Independent

Subsystem: OCC **-** Manage Servers

Symptom: When you upload a large file in a custom field to associate the file with a server, you may receive a java.lang.OutOfMemoryError.

Workaround: None. Be cautious when you upload a file in a custom field. Opsware recommends not uploading a large file in a custom field.

Bug ID: 24470

Description: The results of a second server search in a Wizard are displayed in a new window.

Platform: Platform Independent

Subsystem: OCC **-** Wizards

Symptom: In any Wizard, when you search for servers, by clicking the search tab, the search results are displayed in the same window. When you perform a second search, the search results are displayed in a new window. This behavior is observed when you access the Opsware Command Center using the FireFox browser.

Workaround: Perform the following steps to display the second server search results in the same window:

1. After you perform the first server search in a Wizard, click the Previous button and then the Next button in the wizard. The Select Server page appears.
2. Select the search criteria. The search results are displayed in the same window.

Bug ID: 25772

Description: A warning dialog appears when you perform an operation on a server from the Manage Server page.

Platform: Platform Independent

Subsystem: OCC **-** Manage Servers

Symptom: When you perform an operation on a server from the Manage Server page, you may see the following warning dialog:

```
You are about to leave a secure Internet connection. It
will be possible for others to view information you send.
Do you want to continue?
```

This behavior is only exhibited when you access the Opsware Command Center using Internet Explorer.

Workaround: To turn off this warning dialog, select the "In the future, do not show this warning." Checkbox and then click the Yes button.

Or

1. Open Internet Explorer.
2. In the Home Page, Select Tools > Internet Options.
3. In the Internet Options page, click the Advanced tab.
4. Uncheck “Warn if changing between secure and not sure mode.”.
5. Click Apply.

Bug ID: 26120

Description: The Network Reports Links is not visible under Reports in the navigation panel after Data Center Intelligence Reporting (DCI) is installed.

Platform: Platform Independent

Subsystem: OCC - System Configuration

Symptom: The Network Reports Link is not visible under Reports in the navigation panel after Data Center Intelligence Reporting (DCI) is installed.

Workaround: To make the Network Report link visible, perform the following steps:

1. From the Opsware Command Center Home Page, Click Administration > System Configuration from the navigational panel. The System Configuration: Set Configuration parameters page appears.
2. Click Save. The Network Reports link is now visible under Reports in the navigation panel.

Bug ID: 26382

Description: The Opsware Command Center does not allow server groups to be deleted from My Servers page.

Platform: Platform Independent

Subsystem: OCC **-** Server Groups

Symptom: In the Opsware Command Center, you cannot delete server groups from the My Servers Page.

Workaround: None.

You can delete servers from the Manage Servers Page. To delete a server group, perform the following steps:

1. In the Manage Servers Page, click the check box next to the server group you want to delete.
2. From the Edit menu, choose Delete Group. A confirmation message appears, detailing the number of servers and server groups in the server group that you want to delete.
3. Click OK to complete the deletion of the server group.

The screen refreshes, showing the list of servers and groups without the deleted server group.

Bug ID: 27345

Description: Unable to create a Service Level and associate it with Customer = Not Assigned.

Platform: Platform Independent

Subsystem: OCC **-** Service Levels

Symptom: In the Opsware Command Center, the user is unable to create a Service Level and associate the Service Level to Customer = Not assigned.

Workaround: Create a Service Level and associate the Service Level to Customer = Customer Independent. Edit the Service Level and reassign it to Customer = Not assigned.

Bug ID: 27718

Description: Twist exception appears during cloning of servers when the customer and platform on the master server does not match the target server.

Platform: Platform Independent

Subsystem: OCC **-** Manage Servers

Symptom: In the Opsware Command Center when you clone a server, the source server (master server) and the target servers need to have the same platform and the

same customer. A twist exception appears if the master server and the target server do not have the same customer and same platform.

Workaround: Before cloning a server, reassign the customer and platform on the target server to that of the master server.

Bug ID: 27854

Description: Running a communication Test on a server in an unreachable Satellite throws a 5000 error.

Platform: Platform Independent

Subsystem: OCC **-** Communication Test

Symptom: Running a communication Test on a server in an unreachable Satellite and viewing the results of the job leads to the 5000 error:

```
Error Summary
Name: Standard 500 Error
Description: 500 Internal Server Error
Message Text: The server encountered an unexpected
condition which prevented it from fulfilling the request.
Exception Info:
java.util.NoSuchElementExceptionjava.util.LinkedList$List
Itr.next(LinkedList.java:490)
<<< traceback here >>>
```

Workaround: None. It is not possible to retrieve job specific results for a Communication Test for a server in an unreachable Satellite. The results are recorded in the "current" communication test status for a server in an unreachable Satellite, which is visible from the server properties page or from the communication test view in the server list.

Opsware Command Center Client

Bug ID: 24610

Description: The options in the selection criteria for snapshots of a parent directory and child directory will overlay each other.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: When you include a parent directory (with options) in the selection criteria and a child directory (with different options) as additional selection criteria, the parent directory snapshot and the child directory snapshot will overlay each other as one snapshot. This logic also applies to Windows NT ACL collection and content collection options, and Windows Registry content collection options. How selection criteria for a parent and child directory will overlap is best explained by the following examples.

Consider the following file system, where an ending "`/`" represents a directory:

```
/cust/app/bin/
/cust/app/bin/file1
/cust/app/bin/conf/
/cust/app/bin/conf/conf1
/cust/app/bin/conf/conf2
/cust/app/bin/conf/dev/
/cust/app/bin/conf/dev/conf3
```

Example A

If you create a snapshot using the following two selection criteria:

Directory `/cust/app/bin` (recursive, no checksum)
Directory `/cust/app/bin/conf` (not recursive, checksum)

The snapshot will record the following file system information:

`/cust/app/bin/` (directory)
`/cust/app/bin/file1` (no checksum)
`/cust/app/bin/conf/` (directory)
`/cust/app/bin/conf/conf1` (*checksum*)
`/cust/app/bin/conf/conf2` (*checksum*)
`/cust/app/bin/conf/dev/` (directory)
`/cust/app/bin/conf/dev/conf3` (no checksum)

As you can see, even though `/cust/app/bin` was recursive and had no checksum, the `/cust/app/bin/conf` directory overrode it and all files in that directory have checksums recorded for them.

Example B

If you create a snapshot using the following two selection criteria (by switching the options used in Example A):

Directory `/cust/app/bin` (recursive, checksum)
Directory `/cust/app/bin/conf` (not recursive, no checksum)

The snapshot will record the following file system information:

`/cust/app/bin/` (directory)
`/cust/app/bin/file1` (checksum)
`/cust/app/bin/conf/` (directory)
`/cust/app/bin/conf/conf1` (*no checksum*) `/cust/app/bin/conf/conf2` (*no checksum*) `/cust/app/bin/conf/dev/` directory
`/cust/app/bin/conf/dev/conf3` (checksum)

Example C

If you create a snapshot using the following three selection criteria (by adding a file option):

Directory `/cust/app/bin (`recursive, checksum)
Directory `/cust/app/bin/conf` (not recursive, no checksum)
File `/cust/app/bin/conf/conf1` (checksum)

The snapshot will record the following file system information:

`/cust/app/bin/` (directory)
`/cust/app/bin/file1` (checksum)
`/cust/app/bin/conf/` (directory)
`/cust/app/bin/conf/conf1` (*checksum*)
`/cust/app/bin/conf/conf2` (no checksum)
`/cust/app/bin/conf/dev/` directory
`/cust/app/bin/conf/dev/conf3` (checksum)

In this example, the very detailed selection criteria for `conf1` override the `/cust/app/bin/conf` selection criteria.

Bug ID: 25904

Description: Unable to launch a remote terminal for servers that are running Unix and Windows operating systems.

Platform: Platform Independent

Subsystem: OCC Client **-** Global Shell

Symptom: When you try to launch a remote terminal from the Servers list window in the OCC Client, you will see a telnet session that briefly displays `connecting to 127.0.0.2`… and then closes.

Workaround: This is a bug in WindowsXP SP2. You must install the hotfix that is available at http://support.microsoft.com/default.aspx?kbid=884020.

Bug ID: 26033

Description: The following (example) warning occurs when you create a snapshot using selection criteria that includes the Documents and Settings directory, and files in that directory:

```
Unable to checksum C:\Documents and
Settings\LocalService\NTUSER.DAT: [Errno 13] Permission
denied:
'C:\\Documents and Settings\\LocalService\\NTUSER.DAT'
```

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: When you include the Documents and Settings directory (and files in that directory) in your file system selection criteria, the snapshot will be created with an `Unable to checksum C:\Documents and Settings…` warning.

Workaround: Server Compliance does not support the ability to read the contents of this file. Content for these types of files will not be recorded in a snapshot. Add exclusion rules in your selection criteria to filter out these types of files.

Bug ID: 26121

Description: The audit progress bar may not display correct information about the process completion.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: The audit progress bar displays that the process is 100% complete when it is still taking snapshots of targets.

Workaround: Refer to the status message to determine the status of an audit process.

Bug ID: 26858

Description: An `UnmarshalException` error occurs when the amount of data that is sent to the OCC Client causes the OCC Client to run out of memory.

Platform: Platform Independent

Subsystem: OCC Client **-** Audit & Compliance

Symptom: When you create a package that uses a snapshot (of HKEY_LOCAL_MACHINE and additional files) as the source, and you try to expand the Windows Registry in the Create Package (Details tab) window, Visual Packager displays the following error: `UnmarshalException`.

Workaround: Specify selection criteria that will collect fewer objects. For example, select only parts of the file system and not the entire file system of a target.

Bug ID: 27073

Description: Audit results will be incorrect if you re-run the same audit after performing a Copy To.

Platform: Platform Independent

Subsystem: OCC Client **-** Audit & Compliance

Symptom: You audit the file system of two live servers that are running SunOS5.9. In the Audit Result Browser, you see that a file exists Only on Source. You use the Copy To action to copy a file to the target server. When you re-run the same audit, the results display the same differences with one less difference Only on Source and one more difference On Both But Different. When you view the results that are On Both But Different, you will not see the copied file as the difference. Instead, that file's parent directory is listed as the difference, which is misleading. For example, before the Copy To, the file is ID 1060666. After the Copy To and after you re-run the audit, the audit results refer to this file as ID 1070666.

Workaround: None.

Bug ID: 27211

Description: Opening multiple OCC jobs from the OCC Client causes the job to open in the last active browser window.

Platform: Platform Independent

Subsystem: OCC Client

Symptom: When you open a job created in the Opsware Command Center (OCC) from the Opsware Command Center Client (OCC Client), the job is displayed in the last active browser window.

Workaround: None.

Bug ID: the

Description: Invoking OCC Client Help causes Online Help to open in last active browser window.

Platform: Platform Independent

Subsystem: OCC Client

Symptom: When you invoke Opsware Command Center Client Help, the Online Help is displayed in the last active browser.

Workaround: None.

Bug ID: 27276

Description: A `serverCompliance.FailedToExtractContents` error occurs when you try to create a snapshot or perform an audit using selection criteria that includes a file that has an encrypted attribute.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: When you try to create a snapshot or perform an audit that includes an encrypted file in the selection criteria, you will get a `serverCompliance.FailedToExtractContents` error when you try to browse the snapshot or audit results.

Workaround: Server Compliance does not support encrypted files. Content for these types of files will not be recorded in a snapshot or in audit results. Add exclusion rules in your selection criteria to filter out these types of files.

Bug ID: 27454

Description: In the audit results of a file and directory comparison, an inherited permission does not accurately display.

Platform: Platform Independent

Subsystem: OCC Client **-** Audit & compliance

Symptom: In the audit results of a file and directory comparison, if the permission is an inherited permission from an ancestor of the parent (that is a grandparent, great grandparent, and so on), it does not accurately display.

Workaround: Use the Remote Terminal in the OCC Client to display the permissions for the object in question.

Bug ID: 27530

Description: Deploying an Opsware Agent using the Opsware Discovery and Agent Deployment feature fails when you log in as a sudo user for whom password authentication is not required.

Platform: Platform Independent

Subsystem: OCC Client **-** Opsware Discovery and Agent Deployment

Symptom: When you attempt to deploy Opsware Agents using the Opsware Discovery and Agent Deployment feature by logging in as a sudo user for which password authentication is not required, the following error occurs:

```
Could not enter root password.
```

Workaround: Log in as a user for which authentication is required, or log in as the root user.

ID: 27693

Description: Pushing an application configuration to a server can timeout when the template runs as a post-install script that reboots the server.

Platform: Independent

Subsystem: OCC Client **-** Application Configuration Management

Symptom: Pushing an application configuration to a server can fail when it contains a post-install script (like the one below) that reboots the server:

```
@!filename-key=/arnold/hosts/post.bat@
@!filename-default=/c/tmp/post.bat@
echo "post.bat"
%SystemRoot%\system32\tsshutdn 0 /REBOOT /V
```

The push fails because the reboot exceeds the four minute timeout set for Application Configuration. The error is not reported back to the job dialog window. The job proceeds until it times out.

Workaround: In the post-install script, specify the server to reboot asynchronously, and the job will succeed.

Bug ID: 27733

Description: A `java.lang.outofMemory` error occurs when you try to browse a snapshot that contains too many Windows Registry keys.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: A `java.lang.outofMemory` error can occur for many different reasons, the most common reason is because the snapshot is too large. The Java Console log provides more detailed information about an error that occurs during snapshot parsing.

Workaround: Shut down the OCC Client, and restart it.

Bug ID: 27750

Description: The Audit Result browser displays a Null pointer exception error dialog when you use the object browser to view a file or directory that does not have user or user group attributes.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: You perform an audit on two live servers. In the Audit Result browser, one of the files is recorded as On Both but Different because the group permissions are different. When you click on the file and select Open from the context menu, Server Compliance displays a Null pointer exception.

Workaround: None.

Bug ID: 27806

Description: Possible to push an invalid value set from the Opsware Command Center Client to a managed server without a warning.

Platform: Platform Independent

Subsystem: OCC Client **-** Application Configuration Management

Symptom: When you enter an invalid value in a value set editor and perform a push operation, the invalid configuration file is applied to the server or server group.

Workaround: None. Verify the values you enter in the value set editor before you perform a push operation.

Bug ID: 27858

Description: In the Audit Result browser, Server Compliance accurately recorded a difference for installed hardware in the On Both But Different tab. In the file object browser, the RAM for both source and target is shown as the same size, even though this information is really different (as it is displayed in blue text).

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: When you perform an audit of two servers using selection criteria that includes installed hardware where the RAM size is different on the source and target, this information is displayed in the file object browser as the same RAM size, even though the RAM size is really different. The OCC Client collects RAM size in bytes and converts it to megabytes (MB). If the RAM size difference is very slight, it will not be recorded as a difference in megabytes, even though there really is a difference in bytes.

Workaround: None.

Bug ID: 27858

Description: In the Audit Result browser, Server Compliance accurately recorded a difference for installed hardware in the On Both But Different tab. In the file object browser, the RAM for both source and target is shown as the same size, even though this information is really different (as it is displayed in blue text).

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: When you perform an audit of two servers using selection criteria that includes installed hardware where the RAM size is different on the source and target, this information is displayed in the file object browser as the same RAM size, even though the RAM size is really different. The OCC Client collects RAM size in bytes and converts it to megabytes (MB). If the RAM size difference is very slight, it will not be recorded as a difference in megabytes, even though there really is a difference in bytes.

Workaround: None.

Bug ID: 28001

Description: When you use the Copy To action from a Snapshot browser or Audit Result browser to copy a file and directory (with different users and user groups) from one Unix server to another Unix server, the same user name (uid) is displayed for both the source and target.

Platform: Platform Independent

Subsystem: OCC Client **-** Audit & Compliance

Symptom: If you use the Copy To action to copy the following source file:

```
-rw-r--r-- 1 qatest qatest 46 Jun 9 21:29 first.txt
```

to a target file that is:

```
-rw-r--r-- 1 root other 24 Jun 9 17:52 first.txt
```

you will see the uid (instead of the group name) displayed as the following file:

```
-rw-r--r-- 1 101 qatest123 46 Jun 9 21:29 first.txt
```

When you run the `ls -n` command, you will see that the uid is the same for both the source and the target. In this example, `qatest123` has the same uid of `qatest`.

When you run the `ls -n` command on the source, you will see the following information:

```
-rw-r--r-- 1 101 100 46 Jun 9 21:29 first.txt
```

When you run the `ls -n` command on the target, you will see the following information:

```
-rw-r--r-- 1 101 100 46 Jun 9 21:29 first.txt
```

Workaround: Verify that both servers use the same user name (uid) and group name (gid) mapping.

Bug ID: 28032

Description: Preview differences on imported values for Application Configuration.

Platform: Platform Independent

Subsystem: OCC Client **-** Application Configuration Management

Symptom: If you create an application configuration using the Import Value function and perform a preview for the first time (i.e., the values have not yet been pushed to the server), you may see differences in the preview due to the way the CML parser handles comments in the source configuration file. Once you push the application configuration to a server, the preview differences will no longer show (unless other changes were made).

Workaround: None.

Bug ID: 28054

Description: A deleted and recreated Opsware user is unable to browse the Server Explorer file system in the Opsware Command Center Client.

Platform: Platform Independent

Subsystem: OCC Client **-** Opsware Global File System

Symptom: When the Opsware administrator deletes an Opsware user and recreates the same Opsware user, the recreated user is unable to browse the Server Explorer file system in the Opsware Command Center Client.

Workaround: Restart the Opsware Global File System (OGFS) to disable access to the Server Explorer file system.

Bug ID: 27815

Description: The packaging server for the AIX4.3 operating system was incorrectly configured. The OCC Client erroneously configured a RedHat AS3 server as the packaging server.

Platform: Platform Independent

Subsystem: OCC Client **-** Visual Packager

Symptom: This should only happen if you reinstalled the Opsware System and did not reset the packaging server settings in the OCC Client.

Workaround: When you have a new Opsware installation, you must reset the packaging server settings in the OCC client.

Bug ID: 27833

Description: Creating a package by uploading an installed package or patch does not work for Windows 2000 or 2003 when you do not have the Packages permission.

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Symptom: Invoke the Create Package feature from the Server Browser, snapshot, or audit in the OCC Client. For a Windows 2000 or 2003 server, select packages or patches on the server and click Create. If the packages or patches do not exist in Software Repository, the create package operation will be successful but the OCC Client does not create an application node in the Opsware Command Center.

Workaround: To use the Visual Packager to create Windows 2000 or 2003 packages and upload them to the Software Repository, you must have the Packages user permission in the Opsware System. Contact your Opsware administrator to verify that your user account has this required permission.

Bug ID: 28165

Description: OCC Client fails if you have JRE 1.4.1 installed.

Platform: Platform Independent

Subsystem: OCC Client

Symptom: When you launch OCC Client from a system which has JRE 1.4.1 installed, the following error occurs:

```
An error occurred while launching/running the application.
```

```
Title: OCC Client
Vendor: Opsware Inc.
Category: Download Error

Missing signed entry in resource:
http://occ.brownsox.qa.opsware.com/webstart/xercesImpl.jar
```

Workaround: Java JRE 1.4.2 must be installed on your system to run the OCC Client. You can download this version of Java from http://java.sun.com/j2se/1.4.2/download.html

Packages

Bug ID: 27021

Description: Installation of a latest version of a package does not remove the old version of the package on Windows 2003.

Platform: Windows

Subsystem: Packages

Symptom: When you install the latest version of a package in a Windows server, the older version of the package is not uninstalled automatically.

Workaround: None. Even though the older version of the package is not uninstalled, the latest version is used by the Windows server.

Bug ID: 28064

Description: Package upload fails with a Null Pointer exception for Solaris and Windows.

Platform: Solaris and Windows

Subsystem: Packages

Symptom: In Solaris and Windows, when you upload the following packages from the Packages page, a null pointer exception occurs.

Operating	Package Type

System	
Solaris	Solaris Patch Solaris Patch Cluster
Windows	Windows Hotfix Windows OS Service Pack Windows Utility Microsoft Patch Database

This behavior is only observed in the following cases:

1. If you use the FireFox browser to access the Opsware Command Center.
2. If you set the customer filter to “All Customers” before you upload the packages.

Workaround: You can use any one of the following workarounds:

Use the Upload Patch Wizard to upload a patch, instead of uploading the patch from the Packages page.

Or

Use Internet Explorer to upload packages form the Opsware Command Center.

Or

Set the customer filter to “Customer Independent” and then upload the package from the Packages page.

Patch Management

Bug ID: 22960

Description: The browser stops responding when you upload a patch from the Microsoft Patch Database in the Opsware Command Center.

Platform: Windows

Subsystem: Patches

Symptom: When you upload a patch from the Microsoft Patch Database using the Patch Preference tab in the Opsware Command Center, the browser appears to stop responding. Even though the browser stops responding, the patch is uploaded successfully.

Workaround: None.

Satellite

Bug ID: 27982

Description: `wordbot.unableToCacheFile` error in a Satellite with multiple Software Repository Caches.

Platform: Platform Independent

Subsystem: Software Repository Cache

Symptom: If you have a Satellite that contains multiple Software Repository Caches, and the Satellite is configured for manual updates, you may get the error wordbot.unableToCache file when performing operations that retrieve files from the Cache (for example, when installing software on a server in the affected Satellite). This error occurs when not all of the Software Repository Caches have a copy of every file.

Workaround: When applying manual updates in a Satellite with multiple Software Repository Caches, apply the update to each Software Repository Cache in the Satellite.

Software Provisioning

Bug ID: 26956

Description: A template which is Customer Independent should not be assigned to a customer.

Platform: Platform Independent

Subsystem: Templates

Symptom: In the Opsware Command Center, when you create a template you can select the Operating System version and the Customer for that template. You can also have the server that you apply the template to automatically assigned to the customer associated with the template.
When you create a template that is Customer Independent, select the No option in the Assign Customer field.

Workaround: None.

Web Services Data Access Engine

Bug ID: 27885

Description: Running Distributed Script in the Web Services API fails.

Platform: Platform Independent

Subsystem: Web Services

Symptom: When using the Web Services API to schedule a DSE script execution, if the user password argument is specified in the "open" parameter set object, the operation fails.

Workaround: The user password argument should always be passed in the "hidden" parameter set object.

Documentation Errata

Updates to the Opsware System 5.1 User's Guide

The following topics in the *Opsware System 5.1 User's Guide* are updated with new information.

Permissions Required for Opsware Discovery and Agent "Permissions required for Opsware Discovery and Agent Deployment" in the *Opsware System 5.1 User's Guide*, the user must have the following additional permission to deploy Opsware Agents using the Opsware Discovery and Agent Deployment feature.

Permission	Description
Manage Servers and Groups	View and Manage Servers and groups.

Requirements for Running the OCC Client

The section "Requirements for running the OCC Client" in the *Opsware System 5.1 User's Guide* is updated to include the following information:

Note: When using Internet Explorer, if you try to launch the OCC Client without installing Java J2SE v 1.4.2 JRE, you are prompted to install JRE and run the OCC Client in one step. When you select this option, Java J2SE v 1.4.2 JRE is installed and you get the following error message:

```
Java Web Start –unexpected Error" Unable to launch OCC
Client.
```

To launch the OCC Client, ignore the error message and Click retry.

Opsware Agent Installer Options

The section " Opsware Agent Installer Options" in the Opsware System 5.1 User's Guide is updated with the following information:

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.

During Opsware Agent Uninstallation on a Windows server, the Agent Installer removes the ogshcap.dll file from the following location:

```
%SystemRoot%\system32\ogshcap.dll
```

If the file is open or is in use, the Agent Installer is unable to remove the ogshcap.dll file. The Agent Installer then prompts the user to restart the machine and removes the file after restart.

Updates to the Opsware System 5.1 Configuration Guide

Custom Attributes for Solaris OS Provisioning

In the *Opsware System 5.1 Configuration Guide,* "Sun Solaris Custom Attributes" table should include the following row:

KEYWORD	DESCRIPTION

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.

Using an External LDAP Directory Server with the Opsware System

In the In the *Opsware System 5.1 Configuration Guide*, the section “Using an External LDAP Directory Server with the Opsware System is updated to include the following information:

When setting up delegated authentication with SSL and non-SSL connections to Novell eDirectory, use the following properties in the twist.conf file:

```
aaa.ldap.search.filter.template=(&(objectclass=inetorgperson)(uid=$))
aaa.ldap.search.naming.attribute=uid
```

The example entries in the *Opsware System 5.1 Configuration Guide* are

incorrect.

Contacting Technical Support

To contact Opsware Technical Support:

Phone: +1 877 677-9273 (1-877-Opsware)

E-Mail: support@opsware.com

To Contact Opsware Training

Opsware also offers several training courses for Opsware users and administrators.

Please send a message to training@opsware.com for information.