Opsware® System 4.5, Japanese Edition Release Notes

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

Introduction to Opsware System 4.5, Japanese Edition

Opsware System 4.5, Japanese Edition provides new features, performance enhancements and several bug fixes. This document describes the new features found in this release, and provides information about the most significant bug fixes, and, in some cases, workarounds for known problems.

Two new managed server platforms have also been added:

- Solaris 2.8 and 2.9 for Fujitsu PrimePower

Opsware System 4.5, Japanese Edition includes the following new features:

- Support for DVD-based Installation
- Agent Communication Test
- Agent Uninstaller
- Custom Extension for Server Recertification
- Partial Installation of Solaris Packages
- User Interface Improvements
- Hardware Registration Reliability and Opsware Agent Reporting
- Hardware and Software Registration Efficiency
- Changes to Web Services APIs
- Context-sensitive Online Help

What's New In Opsware System 4.5, Japanese Edition

Agent Communication Test

The new Agent Communication Test in Opsware System 4.5, Japanese Edition enables you to find unreachable Opsware Agents and provides information to help troubleshoot the potential errors.

When you run a Communication Test, the results list all servers with unreachable agents, return specific errors associated with each unreachable Opsware Agent, and provide troubleshooting information to help you get the Opsware Agent back in working order.

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

- **Command Engine to Agent Communication (AGT)** – Determines if the Command Engine can communicate with the agent
- **Crypto Match (CRP)** - Checks that the SSL cryptographic files that the agent uses are valid
- **Agent to Command Engine Communication (CE)** – Verifies that the agent can connect to the Command Engine and retrieve a command for execution
- **Agent to Data Access Engine (DAE)** – Checks whether or not the agent can connect to the Data Access Engine and retrieve its server record

- **Agent to Software Repository Communication (SWR)** - Determines if the agent can establish an SSL connection to the Software Repository
- **Machine ID Match (MID) -** Checks that the machine ID (MID) on the server matches the MID registered in the Model Repository for the agent

See “Communication Test Types” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for information about the various Communication Test types and results.

Communication Test Troubleshooting

One important feature of the Communication Test is to provide troubleshooting information about unreachable servers. For each unreachable server, the nature of the failure is listed by error type in the error details column of the Communication Test window. Context-sensitive Help is available to help you troubleshoot the errors. Clicking the [?] symbol next to the error name provides troubleshooting help for any of the test errors. See Appendix D “Communication Test Troubleshooting” of the Opsware System 4.5, Japanese Edition User's Guide for information about how to troubleshoot Communication Test errors.

Features of the Communication Test

The following features of the Communication Test can help you manage your server more effectively:

- **Running a Communication Test on an individual server -** Allows you to run a Communication Test on an individual server to find out if the Opsware Agent on that server is reachable. See “Running a Communication Test on an Individual Server” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information.
- **Running a Communication Test on multiple servers** – Allows you to run a Communication Test on multiple servers to find out if the Opsware Agent on those

servers is reachable. See “Running a Communication Test on Multiple Servers” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information.

- **Sorting servers by communication status** – Allows you to run a Communication Test to view all managed servers sorted by communication status. For example, you can view managed servers sorted by time, number of errors, OS version, and so on. See “Sorting Servers by Communication Status” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information.
- **Search for unreachable servers** – Allows you to run a Communication Test to view all servers with unreachable agents. See “Searching for Unreachable Servers” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information.
- **Viewing history of all Communication Tests** – Allows you to view the history of all the tests that you run. See “Viewing My Jobs Communication Tests” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information.
- **Exporting unreachable server status list to CSV file format –** Allows you to export the list of all servers listed on a page in the Managed Servers feature of the Opsware Command Center to a Comma Separated Value (CSV) file. See “Exporting Unreachable Server Status List to CSV” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information.

Agent Uninstaller

New in Opsware System 4.5, Japanese Edition is a feature called the Opsware Agent Uninstaller. This new feature:

- Uninstalls and by default, deactivates an Opsware Agent
- Is invokable from the command line or script

- Can be operated unattended because user interaction is not required

In earlier versions of the Opsware System, if an agent needed to be uninstalled, you had to stop manually the Opsware Agent on the server and then delete the agent code on the managed server. In Opsware System 4.5, Japanese Edition, the Agent Uninstaller feature performs these tasks:

- Uninstalls the agent code on the managed server.
- Deactivates the server in the Opsware Command Center and leaves the device record and crypto on the server.
- The Agent Uninstaller does not delete the managed server entry in the Opsware Command Center. However, if you later decide that you no longer want the server to appear in the Managed Servers list, you can delete the server using the Managed Servers area of the Opsware Command Center.

Opsware Agent Uninstaller is run from either the command line or by using a script. See “Uninstalling an Opsware Agent (UNIX and Windows)” in *Opsware System 4.5, Japanese Edition User’s Guide*, Chapter 2 for more information about using this feature.

***Note**: Only use the Agent Uninstaller feature on managed servers. Do not use it on the servers running the Opsware System components. If you do so, the Opsware System services will be non-operational.*

Also note that, on Windows NT platforms, Windows Scripting Host must be installed manually. The Windows 2000 and Windows 2003 operating systems include it automatically.

Custom Extension for Server Recertification

The Opsware agent on each managed server communicates with the Opsware core using crypto material unique to that managed server. The crypto material is assigned

to that server during the installation of the Opsware agent

The Opsware System maintains a record of the crypto assigned to the server. When the agent later communicates with the core, the Opsware system verifies that the crypto provided by the agent to secure the communication link is the crypto assigned to that server.

Occasionally, the need arises to assign new crypto material to one or more managed servers. For example, a system administrator might inadvertently delete the on-disk copy of the server's unique crypto material causing the server to be unable to communicate with the core.

There are other times when the details recorded in the Opsware core of the unique crypto material assigned to a server must be deleted from the record. For example, servers might still have old crypto from a failed crypto upgrade, .or a command like `rm -rf /var/lc/crypto` is erroneously issued as part of an agent upgrade, or the `-c` switch is accidentally passed to the agent installer as part of an agent upgrade.

Server Recert Extension Functionality

The Server Recert custom extension has the following two functions:

- Assign and distribute new crypto material to a server
- Delete the stored details of the crypto material assigned to a server

Assign and Distribute New Crypto Material

When run in this mode, the custom extension script performs the following actions:

- Assigns a new certificate to each of the selected managed servers
- Sends the crypto material to the Opsware Agent on each server for storage locally, and then

- Restarts the Opsware Agent so that it uses the new crypto material from that point forward

Delete Stored Details About Crypto Material

When run in this mode, the script deletes from the Opsware System the details of the server's unique crypto material. This operation has the following two consequences:

- The next time it communicates with the Opsware core, the Opsware Agent on the selected server can no longer proffer the crypto it had previously used.
- New crypto material can later be successfully assigned to the server as a side effect of Opsware Agent installation on the server.

How to Use the Server Recert Extension

The Server Recert Extension is run with the Custom Extension Wizard. For information about running the Custom Extension Wizard, see the *Opsware System 4.5, Japanese Edition User's Guide*, "Running a Custom Extension" in Chapter Ten.

In Step 1 of the wizard, Select Extension, select the Server Recert extension.

When the Wizard completes, review the results. If you are performing a crypto management operation on a large number of servers, you might find it helpful to examine the Failures tab to quickly see any problems.

Partial Installation of Solaris Packages

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 pre-install or post-install 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 or by overwriting it with a new package.

Changes to Web Services APIs

The following changes have been made to the Web Services APIs:

- Operations now use the parameter names in the WSDL, not the generic ones that were generated by early versions of WebLogic

  In Opsware System 4.5, Japanese Edition, WebLogic has been upgraded to version 7.0 SP5. This version of WebLogic provides a workaround for preserving EJB method parameter names in the WSDL file. You will therefore need to change the parameter names used in your client application source code to correspond with the parameter names for each operation as they are now defined in the WSDL, and then re-compile.

- The following class names have been changed:
  - RoleClassNode was changed to Node
  - SoftUnit was changed to SoftwarePackage

  You will need to change these class names in your client application source code to correspond with the new names and then re-compile.

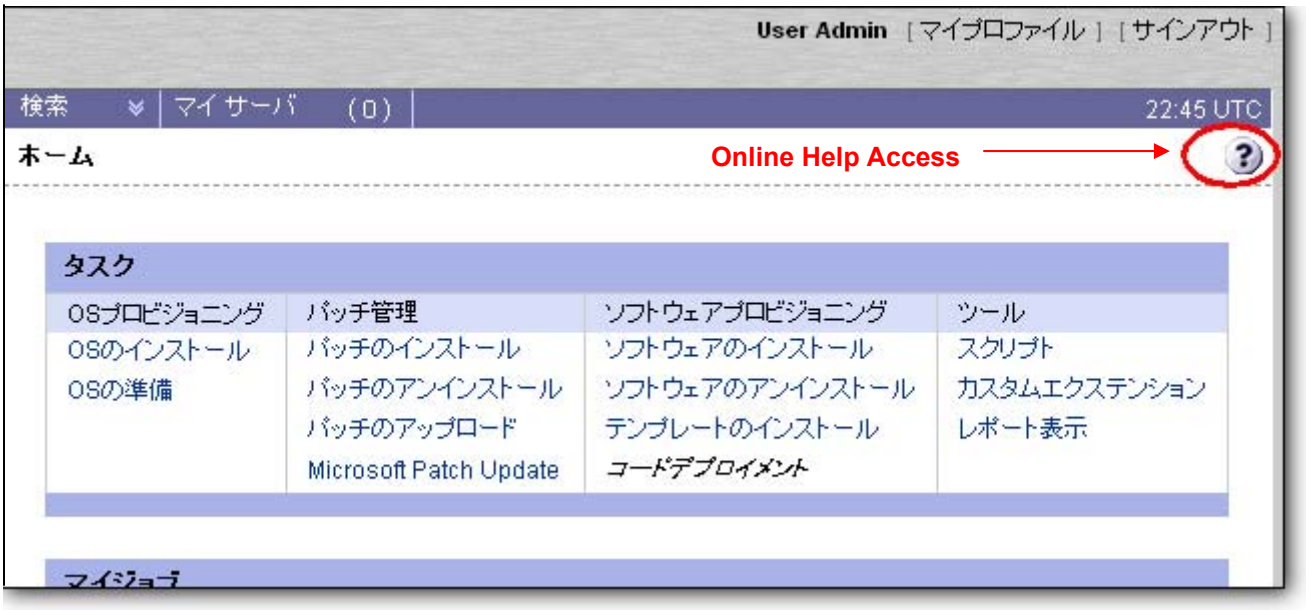
- The name of the Web service has changed:
  - EAIWebService changed to OpswareWebService

  You will need to change the name of the Web service in your client application source code to correspond with the new name and then re-compile.

Context-Sensitive Online Help

Opsware System 4.5, Japanese Edition is the first Opsware System to include online help. The online help consists of the Opsware System 4.5, Japanese Edition User's Guide and Administration Guide.

To access the online help, click the button with the question mark found in the top right corner of the home page.



Because online help is context-sensitive, the topic that you first see when you click the Online Help Access button depends on where you are in the system when you access the online help.

Not all areas of the Opsware Command Center have specific context-sensitive help available. In those cases, clicking the Online Help Access button launches the Help window, where you can use the Contents, Index, or Search tabs to locate topics related to your area of interest.

The following table shows what topic appears when online help is selected from various places in the Opsware System.

Location in the OCC	Default Help Topic
Default Help	Help Home
Home Page	Getting Started with the Opsware System
My Jobs	Scheduling Server Management Jobs
Server Pool	OS Installation with the Opsware Command Center
Managed Servers	Server Management Tasks Related to the Server Life Cycle
Server Groups	Server Groups
Server Search	Ways to Use Advanced Search
Operating Systems	Working with OS Definitions
Patches	Patch Administration Using the Opsware Command Center
Templates	Working with Templates
Packages	Package Management Overview
Scripts	Script Execution Subsystem
Customers	Customer Accounts in the Opsware System
Facilities	Facilities Administration
Applications	Software Tree Overview
Hardware	Overview of Server Asset Tracking
Opsware Software	Opsware Software
Service Levels	Service Levels
IP Ranges	IP Range Groups and IP Ranges
IP Range Groups	IP Range Groups and IP Ranges
CDR Home	Accessing Code Deployment & Rollback
CDR Service Management	Defining a Service
CDR Run Service	Accessing Service Operations in CDR

Location in the OCC	Default Help Topic
CDR Sync Management	Creating and Modifying CDR Synchronizations
CDR Synchronize	Performing Synchronizations and Service Operations
CDR Sequence Management	Defining a Sequence
CDR Run Sequence	Performing Sequences
CDR View History	Viewing Status of Previous Operations
Users & Groups	User Account Administration
Sessions	The Opsware System User Sessions
Server Attributes	Server Properties Overview
System Configuration	System Configuration"
System Diagnosis	Opsware System Diagnosis
Install OS	Ways to Install Operating Systems on Servers
Prepare OS	Defining an Operating System
Install Patch	Installing Operating System Patches Using the Install Patch Wizard
Uninstall Patch	Uninstalling Operating System Patches Using the Uninstall Patch Wizard
Upload Patch	Uploading a Patch Using the Upload Patch Wizard
Microsoft Patch Update	Uploading the Microsoft Patch Database
Install Software	Installing Software Using the Install Software Wizard
Uninstall Software	Uninstalling Software Using the Uninstall Software Wizard
Install Template	Installing Templates Using the Install Templates Wizard
Run Distributed Scripts	How to Execute a My Script or a Shared Script
Run Custom	Opsware Custom Extensions

Location in the OCC	Default Help Topic
Extension	
Reconcile	Overview of the Reconcile Software Wizard
Multimaster Tools	Multimaster Mesh Administration
Configuration Tracking	Automated Configuration Tracking

Searching in Japanese

When using the Search function in Japanese online help, please be aware of the following limitations:

Whenever Kanji or Hiragana is used, there must be a space between every character. For ASCII and Katakana characters, there does not need to be a space between every character, but you must put a space to separate groups of characters from other types of characters. So, for instance,

in this example:

対応するOS上でのリコンサイル

which consists of ASCII, Katakana, Hiragana, and Kanji characters, you must

- put a space after the ASCII characters OS
- put a space after the Katakana characters リコンサイル
- put a space between each of the Hiragana characters する and での
- put a space between each of the Kanji characters 対応 and 上

the resulting search string would look like this:

対 応 す る OS 上 で の リコンサイル

We recommend that Windows XP users install the most recent service pack for XP. Make sure that you have at least Service Pack 2 installed, which contains upgrades to Internet Explorer 6.0.

Also, in the Application Search function in the Opsware Command Center, when a search string contains Half-Width Katakana, a Double-Byte Space, or Kanji characters, you must put an asterisk (*) before and after the search string.

Special Note About Japanese Versions

There are a couple of issues regarding the installation of Japanese versions of packages versus English versions.

- When downloading mbsacli.exe for Windows, be sure to download the English version, not the Japanese version. The Japanese version will not work correctly with the Opsware System.
- Even though the name and version of the Solaris operating system is the same on both Sun Solaris servers and Fujitsu Solaris for Primepower servers, the content of the media for installing those operating systems is different.

  Sun produces the Solaris media for Sun servers, and Fujitsu produces the Solaris media for Primepower servers. The Fujitsu version contains Fujitsu hardware customizations that the Sun version does not.

  The Opsware System creates a filename for each package uploaded during import media. The format for that filename is a unique combination of package name plus version plus architecture, which prevents multiple identical packages from being uploaded.

However, because Fujitsu Solaris for Primepower has packages with the same name, version, and architecture as the corresponding package for Sun Solaris, and because Opsware only allows packages with unique “name plus version plus architecture” combinations to be uploaded, only the first package will be uploaded.

- If you have both English versions of Windows and Japanese versions of Windows on the same mesh, you will not be able to use the Patch Management function.

Non-Localized Areas of the Opsware Command Center

The following areas of the Opsware Command Center have not been localized in Japanese in this release of the Opsware System:

- OK and Cancel buttons – based on the local operating system
- The Opsware logo
- All error pages
- Software Icons with English characters in them: Operating System, Patch, and Application icons
- Wizards' progress bar messages (except Prepare OS and Patch Upload wizards)
- System Configuration: name and description of configuration values
- Users & Groups: Group feature and other permissions
- Server History entries
- Custom extensions not specifically developed for Japanese customers
- Attributes of objects modeled within Opsware
    - Servers
        - Opsware lifecycle

    - Agent status
    - Deployment stage (default values only)
    - Server use (default values only)
  - IP Ranges
    - Subtype
  - Code Deployment and Rollback
    - Service commands
    - Progress messages
  - Patches
    - Patch status
- Data Center Intelligence
- Root node names (e.g. Web Servers, Application Servers, etc.)
- Empty field values: the string (not set) is shown

Supported Operating Systems, Package Types, and File Types

The following table shows the operating systems, package types, and file types that Opsware System 4.5, Japanese Edition supports. Unless otherwise noted, the product runs on both the English-US and Japanese versions of these platforms.

Operating System and Version	Package Type	File Types
SPARC-processor-based hardware (sun4u, sun4us)		
SunOS (2.6,7, 8, 9)	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, Enterprise Server 3.0, WS 3.0)	RPM	.rpm
SUSE LINUX (Enterprise Server 8, Standard Server 8	RPM	.rpm
Microsoft Windows (NT Server 4.0, Windows 2000 Server Family, Windows Server 2003 Family)	Hotfix	.exe
	Service Pack	.exe
	MSI	.msi
	ZIP	.zip
	Security Patch	.exe
	Windows Utility	.exe
	Microsoft Patch	.xml, .cab

Operating System and Version	Package Type	File Types
	Database	
IBM-POWER-processor- based hardware		
IBM AIX (4.3.3, 5L V 5.1, 5L V 5.2)	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, 11i	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 10.20 with the Patch Wizard; you can only install them with the Install Software Wizard.*

Supported Browsers

These are the browsers that Opsware System 4.5, Japanese Edition supports.

Browser	Windows 2000	Windows 2003	Windows XP	Linux 6.2+	Sunos 5.6+	Apple os x
Microsoft Internet Explorer 6.0	X	X	X			

Please note that Microsoft Internet Explorer 6.0 is supported on the Windows operating system shown in this table for the Opsware Command Center, however the online help only works with Internet Explorer 6.0 on Windows XP and not on Windows 2000 or Windows 2003.

Supported Core Platforms

You can operate Opsware System cores on SunOS 5.8-J, SunOS 5.9-J, and Red Hat Linux AS 2.1-J.

The Data Center Intelligence Server runs on Windows 2000.

Supported Installations

The Opsware System 4.5, Japanese Edition release supports the following installations:

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

- First time, from-scratch installation of multimaster cores

Updates to the Installation Procedures

To install an Opsware System 4.5, Japanese Edition standalone core or a core in a multimaster mesh, follow the procedures and content as documented in the Opsware *System 4.5, Japanese Edition Installation Guide*, with the following changes as described in these release notes.

Specifying a Locale

Before you install components on a server, the Opsware Installer interviews you for information about how you will install the Opsware core in that facility.

Opsware System 4.5, Japanese Edition supports installing the Opsware System with either the English-US or Japanese locale. To set the locale for the Opsware core, enter the locale value at the following prompt during the interview phase of the installation.

PROMPT	DESCRIPTION
Please enter the default locale for users of the Opsware Command Center (en/ja) (Parameter: default_locale)	Specifies the default locale (language, character sets, and date and time formats) for the Opsware System core. Source: Arbitrary (however, Opsware System 4.5, Japanese Edition only support the English-US and Japanese locales) Example: `en` or `ja`

This table updates the topic “Description of Required Information for Installation” in Chapter 3 in the Opsware System 4.5, Japanese Edition Installation Guide to include this new prompt.

Installing the Opsware Command Center Help

The Opsware Installer installs the English and Japanese versions of the Help. When a user logs into the Opsware Command Center and clicks the Help icon, the Opsware Command Center displays the Help in English or Japanese depending on the locale of the Opsware core or the locale setting in the user's profile.

In Opsware System 4.5, Japanese Edition, the Opsware Installer menu includes a selection to install the Opsware Command Center Help. When installing a standalone core or a core in a multimaster mesh, select the "Opsware Documentation" component to install online help.

Requirements for installing the Opsware Documentation component:

- You *must* install the Opsware Documentation component on the server where you install the Opsware Command Center component.
- Install the Opsware Documentation component *before* you install the Opsware Command Center component. (If you install the documentation after installing the Opsware Command Center, you must restart the Opsware Command Center component.)

This topic updates the following topics in the *Opsware System 4.5, Japanese Edition Installation Guide*:

- Step 11 in the topic "Installing a Standalone Core" in Chapter 5
- Step 18 in the topic "Adding a Third Core or More to an Opsware Multimaster Mesh" in Chapter 8

Documentation

This release comes with the following documentation:

- *Opsware System 4.5, Japanese Edition Release Notes*
- *Opsware System 4.5, Japanese Edition Upgrade Guide*
- *Opsware System 4.5, Japanese Edition Installation Guide*
- *Opsware System 4.5, Japanese Edition User's Guide*
- *Opsware System 4.5, Japanese Edition Administration Guide*
- *Version 1.0.3 Data Center Intelligence Administrator's Guide*

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

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

Known Problems, Restrictions, and Workarounds in Opsware System 4.5, Japanese Edition

Users should be aware of the following known problems in Opsware System 4.5, Japanese Edition.

Code Deployment Subsystem

Bug ID: 6160

Description: Symlinks are always synchronized

Subsystem: Synchronization

Platform: Platform Independent

Symptom: Due to limitations of UNIX, when synchronizing a directory, symlinks are always synchronized regardless of whether a change was made. CDS identifies these links in the Preview operation and synchronization results even if they did not change.

Workaround: None

Bug ID: 6181

Description: Timestamp of a directory was not preserved when synchronizing to the Live directory

Subsystem: Synchronization

Platform: Platform Independent

Symptom: Performing a sync-to-live might not preserve directory or sub-directory timestamps.

Workaround: None.

Bug ID: 9863

Description: Error code 111112 appears when synchronization fails between a server not using NAT to one that is using NAT. This error code might also appear for other CDS synchronization errors.

Subsystem: Synchronization

Workaround: Users should not perform synchronizations from a server not using NAT to one that is using NAT.

Bug ID: 12344

Description: Defining a service or a sync directory with a trailing forward-slash causes CDR to think the Windows directory doesn't exist.

Platform: Windows

Symptom: Modifying the live directory defined in the service as, for example, "d:/directory/live/" causes the preview to fail with the following error:

```
"The directory d:/directory/live/ does not exist on the source host."
```

Workaround: Use only trailing backslashes when defining a service or a sync directory. Naming directories with a trailing backslash won't cause a failure. For example, change the above live directory in the service definition to be "d:\directory\live\" and the preview will succeed.

Bug ID: 14295

Description: Able to disable the 'Code Deployment' checkbox.

Platform: Platform Independent

Subsystem: Server Attributes

Symptom: You can uncheck the 'Code Deployment' box in a Use value that is assigned to a server in a CDR service/synchronization definition.

Workaround: None

Bug ID: 15714

Description: A JavaScript error appears if the entry in the Extra Instruction field in the Code Deployment and Rollback system exceeds 10kb of data.

When the user sends a request for a service to be performed and adds more than 10kb of text to the Extra Instruction field, a JavaScript error appears when the Run button is clicked.

Platform: Independent

Subsystem: Code Deployment & Rollback

Workaround: Enter fewer than 10,000 characters in the Extra Instruction field.

Bug ID: 16078

Description: Unable to save a Sequence due to size limit. Attempting to save a CDS sequence with 21 multi-byte characters in the name failed with an ambiguous message.

Platform: Platform Independent

Subsystem: Code Deployment & Rollback

Workaround: This should not occur as long as the Oracle database has been correctly configured to use character semantics instead of byte semantics.

Bug ID: 19623

Description: A 500 error was encountered when attempting to use a new managed server for Code Deployment before hardware registration of that server was complete.

Platform: Platform Independent

Subsystem: Code Deployment and Rollback Subsystem

Workaround: The first full registration of the server is performed by the Opsware Agent within an hour of being installed. Allow registration to complete before using the server.

Command Engine (Way)

Bug ID: 17672

Description: The Opsware Command Center allows any users to be deleted when in fact some users should never be deleted. For example, certain users such as “admin” have special Command Engine privileges that when deleted can cause problems accessing access the Command Engine. (Also, do not delete the last user in the Command Engine’s (Way’s) master-admin role, because the admin user is usually the only user in that role.)

NOTE: a user having Command Engine admin privileges has nothing to do with user with Opsware Command Center admin user privileges. Any Opsware Command Center users can have Command Engine admin privileges. The Opsware Command Center cannot tell which users can be deleted without affecting the Command Engine.

Platform: Platform Independent

Subsystem: Command Engine

Workaround: None

Configuration Tracking Subsystem

Bug ID: 9283

Description: Permissions and timestamps not restored from the directory backup objects

Platform: Platform Independent

Symptom: When restoring the permissions and timestamps of a directory object over an existing directory, the system does not restore the permissions and timestamps.

Workaround: None

Bug ID: 15901

Description: Reconciling directory tree policies with trailing backslashes fails

Platform: Windows

Error Message: Opsware Error: Failed To Verify Configuration Tracking Policy failed on server m107core0.cust.custqa10.com

Workaround: To avoid this problem, do not use a trailing slash in the backup policy.

Bug ID: 18108

Description: If you install IIS on a Windows 2003 server without restarting the agent, then create and reconcile a Configuration Tracking backup policy onto the server, the Configuration Tracking Subsystem will abort during the reconcile preview with this error: "IIS not found." Note that the installer never prompts the user to reboot the server.

Platform: Windows 2003

Subsystem: Configuration Tracking

Error Message: IIS was not found

Workaround: Restart the agent to ensure that IIS is detected.

Bug ID: 20820

Description: After disabling a Configuration Tracking policy entry with Japanese characters, the disabled entries appear under both the Enabled as well as Disabled lists. They should appear only under the Disabled list. The characters under the Disabled list display as "???" in place of valid Japanese characters.

Platform: Platform Independent

Subsystem: Configuration Tracking

Workaround: None

Data Access Engine (Spin)

Bug ID: 17953

Description: Modifying the Windows system hostname does not update the NetBios hostname. Using the Opsware System to modify the Windows Computer name field only modifies the system hostname and leaves the NetBios hostname unchanged.

Manually updating the Windows system hostname automatically updates the NetBios hostname.

Platform: Windows

Subsystem: Data Access Engine

Workaround: None

Script Execution Subsystem

Bug ID: 16305

Description: In the Run Distributed Script wizard, if you select a script whose name has a trailing backslash, the Next button is not enabled, and you won't be able to continue.

Platform: Platform Independent

Workaround: Follow these steps:

1. Select a script with no trailing backslash in the name. This enables the Next button.
2. Select the script with the trailing backslash in the name.
3. Now that the Next button has been enabled, you can deselect the script you first selected.

Network Configuration

Bug ID: 14236

Description: Network Configuration doesn't report the gateway for DHCP-managed Red Hat Linux servers. The Gateway field under the Network tab is blank for a Linux server that is managed by DHCP.

Platform: Red Hat Linux

Workaround: This missing Default Gateway data has no negative effect on the operation of the managed server or Opsware. Do not set a value in this field, if the value assigned by DHCP is known.

Bug ID: 17916

Description: An update to enable a second interface failed, and then the settings for the second interface reverted to the same settings as the first interface.

Platform: Solaris

Subsystem: Network Configuration

Workaround: Be sure that host names are unique.

Bug ID: 17925

Description: Changing interface from static to DHCP failed, but the server remains reachable.

Platform: Platform Independent

Subsystem: Network Configuration

Error Message:

```
"New network configuration could not be verified"
```

Workaround: None

Bug ID: 17949

Description: Changing interface from static to DHCP on AIX doesn't work. The server reboots, but when it comes back up, its interface is still set to the old static configuration.

Platform: AIX

Subsystem: Network Configuration

Workaround: None

Bug ID: 17950

Description: Changing interface from static to DHCP on HP-UX fails. The interface is correctly set to DHCP, but after the server reboots, the Opsware System is not able to verify the configuration and the update fails.

Platform: HP-UX

Subsystem: Network Configuration

Workaround: None

Bug ID: 18868

Description: The Linux agent is only able to detect the presence of the gateway specified in /etc/sysconfig/network if the value for the gateway is also present in /etc/sysconfig/network-scripts/ifcfg-eth0. If this is not the case, the agent reports nothing during Hardware Registration, which is problematic because the Gateway field is mandatory on the Network tab for Server properties. When no gateway is reported by the hardware registration process, an error is generated when changes are saved on the network tab.

Platform: Red Hat Linux 8.0

Subsystem: Opsware Command Center

Workaround: None available.

Bug ID: 19469

Description: Disabled interfaces do not display in the Opsware Command Center.

Platform: Windows

Subsystem: Network Configuration Backend

Workaround: In order for a network interface to be managed by the Opsware System, it needs to be enabled. To do this:

1. Open the Network Connections dialog in Control Panel.
2. Select the disabled interface.
3. Right click, and select "Enable" from the pop-up menu.

Bug ID: 19820

Description: Attempt to disable a second interface fails with the following error:

```
Error Summary
Name: New network configuration could not be verified
Description: The server's network configuration is not as
expected after a reboot. Most likely, the new configuration
prevented contact with the Opsware core and the server was
reverted to the previous configuration.
Error Details
Error ID: 64310100
Time: 07/14/04 00:09:48
Hostname: m072.qa.opsware.com
Reverted configurations: interface en1 boot_proto
```

Platform: AIX 5.1

Subsystem: Network Configuration Backend

Workaround: None available. You cannot disable AIX network interfaces using the Opsware System.

Opsware Agent (Cogbot)

Bug ID: 9433

Description: Agent backup process continues during timeouts in the Configuration Tracking Subsystem.

Platform: Platform Independent

Subsystem: Opsware Agent

Symptom: If a Restore operation times out during the pre/post restore backup phase because the Package Repository hangs, the Command Engine session times out but the backup operation remains in progress. Eventually, that operation times out, but only after a long time (up to 1 hour). Meanwhile, all the Configuration Tracking Subsystem-related operations initiated by the user, such as manual backup,

reconcile, restore, and enable/disable backups, result in an “acsbar.RunInProgress opsware” error.

Workaround: None

Bug ID: 9519

Description: Agent Installer –settime option may lead to a fatal error.

Platform: Platform Independent

Subsystem: Agent

Symptom: The --settime (-t) option of the Opsware Agent Installer is used to synchronize the clock of the machine the agent is installed on with that of the Opsware core. If the machine on which the agent is being installed is significantly ahead of the clock on the core, the clock on the managed server is set back in time. This scenario can be fatal on Solaris machines (for example, if jobs stop working until cron is restarted, or the machine is rebooted).

Note that this scenario could happen both on newly installed machines and on assimilated servers. In both cases the result is fatal.

Workaround: Do not use the --settime option unless you are sure the above scenario is not a problem to you. In addition, you can create a code change that "back-dates" all generated certificates by 24 hours, that is, make the "valid-from" date on the certificate the current core time minus 24 hours, to make sure that there is a significant time window for Agents that might be out of sync with the core. If a managed server is more than 24 hours behind the core time when an Agent is installed (and the --settime option is used), registrations will fail until the managed server clock catches up.

Bug ID: 9655

Description: Opsware Agent backward compatibility message should provide more specific information. If a new version of the Opsware System is installed and the Opsware Agent on a server is not upgraded to match the new version, the new features of the Opsware System are not available on the servers with the older agents. If a user attempts to use new features on a server with an older agent, the

error message does not provide enough information for the user to understand the problem. When attempting to use Opsware Configuration Tracking, for example, on a server with an agent that does not support this feature, the Opsware System returns the following message.

Text:

```
An unexpected error occurred while updating the configuration
tracking policy stored on the server.
acsbar.setbarbotstate
```

Workaround: None

Bug ID: 10842

Description: The daemonbot.err log file is not capped or rotated the way other files are (other files typically have a maximum size and a maximum number of retained versions). This log file could potentially fill up a disk.

Workaround: Monitor this log file and rotate manually as needed to manage its size.

Bug ID: 13971

Description: If the Opsware Agent's configuration is changed via the Opsware Command Center, the changes will not take effect on an individual server unless it has been restarted twice.

Platform: Independent

Workaround: Restart reboot the agent twice any time that you make a change to the agent configuration via the Opsware Command Center. Also, if the Agent configuration has been changed from the default, when assimilating a server, you will have to manually restart the agent after it's installed before the custom configuration will take effect. Servers provisioned using the OS Provisioning function will also need to have their agents restarted.

Bug ID: 14186

Description: x86 Opsware Agent doesn’t report a serial number unless SMBIOS type 1 serial number is present.

Platform: Windows, Linux

Subsystem: Opsware Agent

Symptom: The agent on x86 platforms only reports a serial number if the SMBIOS type 1 (System Information) serial number is present. On some platforms, such as the Dell 1650, the Type 1 serial number is absent.

Workaround: None

Bug ID: 14445

Description: The Agent Installer fails when the –template option is used with the full name of the template.

Platform: Independent

Workaround: Use the template ID number instead of the full template name.

Bug ID: 17060

Description: When NFS is enabled, and HP-UX servers are rebooted as part of the process of reverting from a bad network configuration, the server does not return from the reboot.

Platform: HP-UX

Subsystem: Opsware Agent

Bug ID: 17507

Description: Errors returned on Windows NT4 when IP addresses have certain characteristics. The problematic IP addresses are those with a zero in any of the four bytes. For example: 10.252.0.244 will fail while 10.252.1.244 will work.

Platform: Windows NT4

Subsystem: Opsware Agent

Workaround: None available. The most likely explanation for the problem is that Microsoft developers misinterpreted the RFC that states that no address or subnet shall be zero, interpreting it to mean 'no octet shall be zero'.

Bug ID: 18598

Description: Agent does not check disk space before downloading.

Platform: Windows

Subsystem: Opsware Agent

Workaround: None available.

Bug ID: 19923

Description: Windows NT Agent Uninstaller does not work if WScriptHost is not installed.

Platform: Windows NT

Subsystem: Opsware Agent

Workaround: Windows NT servers must have Windows Scripting Host 5.1 and Internet Explorer 5.5 installed.

Opsware Command Center

Bug ID: 7363

Description: Uploading a file fails and displays an error but Opsware Command Center still displays the package in the UI

Platform: Platform Independent

Symptom: A user uploads a file to Opsware Command Center. The upload fails and Opsware Command Center displays the error "Unknown Package Repository Error" at the end of the upload process. The user then searches for the package and the package appears in Opsware Command Center. The package was successfully uploaded to a /temp directory; however, when the Package Repository tried to move the package to the correct directory the move failed. Therefore, the package was successfully registered with the Truth database but does not exist on the Package Repository.

Workaround: This situation rarely occurs. However, if this situation occurs, delete the file by using Opsware Command Center, and then re-upload the file.

Bug ID: 7889

Description: History is not generated for Roles in the Customer, Facility, and Hardware Role Types

Platform: Platform Independent

Subsystem: Nodes in the Opsware Command Center

Symptom: When the Roles in the Customer, Facility, and Hardware Role Types are updated events do not appear under the History tab.

Workaround: The user can track these changes in other ways. For example, by using the custom attributes of the Roles. Make the attribute name equal the date or name of the change, and the value equal to the changes made and who made the changes. The user can track the changes in a log or spreadsheet.

Bug ID: 8058

Description: Package information might not reflect the package the user downloads

Platform: Platform Independent

Subsystem: Manage Packages

Symptom: User-A uses Opsware Command Center in Facility-1 to download a package. User-A has problems with the package and asks User-B to build a new package. Using the Opsware Command Center in Facility-2, User-B uploads the new package to the Package Repository in Facility-2 and updates the meta-information about the package (such as the description and notes). User-A logs into the Opsware Command Center in Facility-1 and navigates to the package. Seeing the new description, notes, and timestamp, User-A downloads the package to User-A's local disk. User-A downloaded the original file, not the modified version described by Opsware Command Center. This situation occurs because User A downloaded the original file before and the Opsware system in Facility-1 cached the file locally. The TTL was not expired for the package, so Opsware Command Center downloaded the cached copy of the package.

Workarounds:

Perform either of the following workarounds.

- Wait for the specified Package Repository cache timeout period.

- Upload the package to the Package Repository in the same facility as the Opsware Command Center instance being used.

Bug ID: 8450

Description: Deleting a package that has been installed by reconciling a device causes the subsequent reconcile to fail.

Platform: Platform Independent

Symptom: Reconcile fails.

```
Name: Error in parsing package name.
Description: This may mean the Opsware Agent is an old version or the
package:/packages/loudcloud/HP-UX/11.00/PHCO_27012.depot/PHCO_27012.CMDSAUX-1.0 is not properly registered with Opsware.
```

Workaround: Do not delete packages unless they have not been used. You can upload the package back to the Package Repository to clear this problem. See Chapter 4, “Uploading a Package” in the Opsware System 3.6 User’s Guide for information.

Bug ID: 8922

Description: Source always reflects top level node (Role Class Stack) when target is the same within a hierarchy of nodes

Platform: Platform Independent

Symptom: After reconciling the policies and then clicking on Backup Policy under the Backups tab of the device, the source displayed is the top level Role, even though the device is attached to level3.

Workaround: Go to the Nodes tab of a device and find the actual role in the corresponding role type.

Bug ID: 12178

Description: Script deletion does not clear the name field.

Platform: Platform Independent

Subsystem: Distributed Scripts Execution Subsystem

Symptom: When you delete a distributed script, the name field is not NULL'd, so when you could create a new script you may get a "Script Name not Unique error," due to a conflict with a deleted script.

Workaround: None

Bug ID: 13894

Description: Attempt to delete 499 LPPs fails with an “OCC not available” message.

Platform: Platform Independent

Subsystem: Packages

Error Message:

```
Opsware Command Center is Not Available. The server may
still be starting up. Please retry in a few minutes. If
the problem persists, please contact your local support
personnel for assistance.
```

Platform: Platform Independent

Symptom: When reconciling packages, the Opsware Command Center displays an incorrect number of packages installed when any packages have the "reboot on install" option set. Opsware Command Center displays the number of packages installed since the last reboot, not the total number installed during the reconcile process.

Note: Large operations may take extra time to process. An example is verifying that 500 packages can be deleted. Additionally, some types of packages may take longer to verify than others, such as LPPs, which may take longer to verify than RPMs. Users may encounter a timeout for large operations.

Workaround: None

Bug ID: 14139

Description: Should not be able to Change OS when Tracking Policies are in place.

Platform: Platform Independent

Subsystem: Service Levels

Symptom: When you create a service level node and create tracking policies for it, you may be able to incorrectly modify the OS. When you click on the Configuration Tracking tab, you may see the following (or similar) message:

```
This node cannot have tracking policy because its
associated operating system is OS Independent.
Location: Service Levels
Name: joe-sl-win2003
Description: kajfgkj
Notes:
Customer: Customer Independent
Operating System: Windows 2003
Locked: No
Allow Servers: Yes
ID: 13440001
```

Workaround: None

Bug ID: 14441

Description: Users should not use two or more instances (i.e. identical packages with multiple copies in Opsware) of the same package with the same server. This problem can occur if a user uploads the same package more than once and uses more than one instance on the same server. For example, a user might upload the same Windows Hotfix twice, for two different customers. Problems arise if both of these Hotfixes become attached to, and are installed and reconciled on, the same server. For example, if the user installs a Hotfix and then applies a second instance of the same Hotfix, then an error will occur.

Platform: Independent

Symptom: Package installation displays a traceback error about database constraints

Workaround: Do not attach a server to two different instances of the same package (e.g., a package that has been uploaded twice but for two different customers.) If the problem does occur, make sure to unattach all but one instances of the package and then use the Reconcile Wizard on the server with the "uninstall detached software" option selected. This option will disassociate the server from the package instances that have been unattached.

Bug ID: 14463

Description: In an Opsware Command Center wizard, using the Previous and Next buttons to change the OS version of server or package (OS, application, or patch) does not change the OS version of the corresponding page. For example, you are in the Install Software Wizard, you select a Windows application in the Select Software step. You click the Next button to proceed to the Select Servers step. You select a Windows server, and then deselect the server. You click the Previous button to return to the Select Software step and change the OS version of the software. In the Select Software step, only Windows software is available for selection.

Platform: Platform Independent

Subsystem: Platform Independent

Workaround: Cancel wizard and start over.

Bug ID: 14634

Description: Deleting a server results in a timeout error. Deleting a server can generate a large number of transactions, causing the Opsware Command Center to report a 3100 timeout error. In spite of the error message, however, the server is successfully deleted.

Platform: Independent

Workaround: If you receive a timeout error when deleting a server, check the status of the server again in about 30 minutes. The server should be successfully deleted.

Bug ID: 14864

Description: The Opsware System still 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: Platform Independent

Workaround: By executing multiple reconciles of 50 devices each, you can reconcile, for example, 200 devices at the same time (providing you close the reconcile update windows and follow the progress in the My Jobs list).

Bug ID: 15177

Description: Uploading a script with an apostrophe in the script's name results in an EJBCException.

Platform: Independent

Subsystem: Script Execution Subsystem.

Symptom: Script cannot be uploaded.

Workaround: Do not use apostrophes in any script names.

Bug ID: 15588

Description: Uploading an HP-UX depot to the Software Repository using the Opsware Command Center sometimes fails and no error message is displayed.

Platform: HP-UX

Symptom: HP-UX depot fails to upload.

Workaround: If an HP-UX depot fails to upload through the Opsware Command Center, use the Opsware Command Line Interface to upload the package.

Bug ID: 16070

Description: Encoding scheme needed in script download; currently all script downloads, script results, and CSV information are in UTF-8

Platform: Platform Independent

Subsystem: Opsware Command Center

Workaround: Use the iconv tool on Linux and Unix. For Windows, use the tool found at: http://www.i18nfaq.com/ictool.html
Both of these tools will convert between UTF-8 and national character sets.

Bug ID: 16704

Description: When the Network Property window is left open on a Windows 2003 server, any modifications made on the Network Configuration tab will fail with an ambiguous error message that does not provide enough information to determine the problem.

Platform: Windows 2003

Subsystem: Opsware Agent

Workaround: None. Close the Network Property window before saving the network configuration modifications.

Bug ID: 19879

Description: When a new user is created, it does not appear in the Users and Groups function if there are more than 2000 users defined.

Platform: Platform Independent

Subsystem: Opsware Command Center

Workaround: Edit the file

`/cust/usr/netscape/server4/slapd-cast/config/slapd.conf.`

Change the line

```
sizelimit 2000
```

to

```
sizelimit n
```

where **n** is a number larger than the maximum number of users you intend to create in the Opsware System. Then, restart the Access and Authentication directory with the command

```
/etc/init.d/cast –updown restart
```

Bug ID: 20042

Description: It is possible to start a new Operating System installation before the previous one is complete.

Platform: Solaris 5.8

Subsystem: Opsware Command Center

Workaround: None available. If you know that an installation is in progress, you should wait.

Bug ID: 20053

Description: In a core with 500 or more customers, if you edit existing My Customers records on the home page and then add new customers, the newly-added customers do not appear when you re-display the home page.

Platform: Platform Independent

Subsystem: Opsware Command Center

Workaround: None available. This can only be avoided by not having a lot of customers in the My Customers area of the home page.

Bug ID: 20665

Description: Solaris Patch fails to upload.

During a Solaris patch upload, the following error was returned

```
OpswareError: cogbot.packageError
[ module: solpatch_handler.py,
  method: extractFiles,
  line: 145,
  hostname: m065.dev.opsware.com,
  timestamp: 19/Aug/2004 011910,
  package: /cust/word/tmp/wordbot7/112490-03.zip,
  results: Could not expand file:caution: filename not
matched: 112490-03/README.112490-03,
  command: unzip -qd /cust/word/tmp/wordbot7
/cust/word/tmp/wordbot7/112490-03.zip 112490-
03/README.112490-03 < /dev/null]
```

Platform: Solaris

Subsystem: Software Repository

Workaround: Unzip or untar the file and repackage it as a zip or tar file without the additional directory that the original compressed file contained. For example, if the contents of a zip file are ./112490-03/README.112490-03, you would repackage the zip file so that the contents were ./README.112490-03.

Bug ID: 20731, 20776, 20799, 20830, 20831

Description: When a string is bracketed by less than (<) and greater than (>) symbols the system strips the brackets.

Platform: Platform Independent

Subsystem: Server Attributes, Applications, IP Ranges, Code Deployment, Service Levels

Workaround: If the less than (<) and greater than (>) symbols must be used, create the entry without the brackets. Then, edit the newly-created record and add the brackets.

Bug ID: 20746, 20724, 20744

Description: A custom attribute with a multi-byte name can't be opened or deleted when the name is exactly 50 bytes long, the maximum size for the field.

Platform: Platform Independent

Subsystem: Server Groups, Code Deployment, Customers

Workaround: Limit custom attribute names to fewer than 50 bytes.

Bug ID: 20794

Description: There is no Encoding Scheme for Solaris Package Instance Response Files. Currently, in the Opsware Command Center, you cannot specify an encoding scheme during the upload of a Solaris Package Instance response file. The encoding scheme is necessary because the response file may contain the install directory name, which could be in Japanese.

Platform: Solaris

Subsystem: Package Management

Workaround: Do not use non-ASCII characters in response files. If you need to reference local files whose names have non-ASCII characters, create a symbolic link to these files so that the symbolic link uses only ASCII characters in the file name.

Bug ID: 20835

Description: Patch Preferences pages has Standard 3000 Error.

After uploading the mssecure.xml file from a Japanese server using multibyte characters in the path, the Patch preferences page does not load correctly

Platform: Windows

Subsystem: Opsware Command Line Interface

Workaround: Import mssecure.cab directly into the Opsware system from the mssecure.cab URL provided in the Opsware Command Center. Do NOT download the cab file to a local directory and then import this cab file into the Opsware system.

Bug ID: 20059

Description: In attempting to upload a Solaris Patch Cluster, the Upload Patch Wizard hangs.

Platform: Solaris

Subsystem: Patch Upload Wizard

Workaround: None, however, the file is successfully uploaded and the registration process is in progress. To see if the process is complete, search for that package in the Opsware Command Center.

Bug ID: 20595

Description: Application Search does not Work for Kanji, Half-Width Katakana and Double-Byte Space. Searching for application nodes using Hiragana and Katakana characters works fine. But no results are returned when Kanji, Half-Width Katakana and Double-Byte Space are used.

Platform: Platform Independent

Subsystem: Web Services Data Access Engine

Workaround: Put an asterisk (*)before and after search strings that contain Half-Width Katakana, Double-Byte Space, and Kanji characters.

Opsware Command Line Interface

Bug ID: 19828

Description: When uploading a package to a satellite (remote facility), you do not receive an error message when an invalid value is entered for the Software Repository (word) and Gateway ports.

Platform: Platform Independent

Subsystem: Opsware Command Line Interface

Workaround: None. However, if your package is not successfully uploaded to the satellite, verify the numbers you entered for the Software Repository (word) and Gateway ports on the command line and enter the command again.

OS Provisioning Subsystem

Bug ID: 12500

Description: OS Provisioning does not install Configuration Tracking policies.

Platform: Platform Independent

Subsystem: Provisioning

Symptom: Users can create Configuration Tracking backup policies on the nodes that are used for OS Provisioning, but the policies are not backed up on the server at successful completion. OS Provisioning does a software reconcile only (no backup policy reconcile).

Workaround: None

Bug ID: 12750

Description: OS Provisioning Boot Agent does not survive NFS server reboot.

Platform: Platform Independent

Symptom: Opsware System 4.0 does not have a recovery mechanism for Solaris machines in the "server pool" (i.e., running the miniagent off the miniroot mounted via NFS) if the NFS server goes away (gets rebooted). When the NFS server comes back up, clients receive "stale NFS handle" errors.

Workaround: You must manually reboot the managed server using the

```
boot net: dhcp – install
```

command, which will put it back into the server pool. For more information using this command, see Booting a Solaris Server over the Network in Chapter 4 of the User's Guide.

Bug ID: 14077

Description: Unable to open the passdb database while installing media server.

Platform: Platform Independent

Subsystem: Provisioning

Symptom: While installing a standalone core, the following was output during the media server installation:

```
"unable to open passdb database."
```

The installer continues.

Workaround: You can safely ignore this message.

Bug ID: 15577

Description: If the DHCP server is set up without reverse-resolvable IPs, the server name field for Solaris provisioning will be blank.

Platform: Solaris

Subsystem: OS Provisioning

Workaround: None

Bug ID: 15701

Description: Provisioning of SunOS 5.7, 5.8, and 5.9 fails if the power management cluster (SUNWCpm) is not excluded from the JumpStart profile.

Platform: SunOS 5.7, 5.8, 5.9

Subsystem: OS Provisioning

Resolution: Exclude the power management patch (SUNWCpm) from SunOS 5.7, 5.8, and 5.9 installations.

Bug ID: 17874

Description: MRL is registered with the Model Repository (Truth) despite the fact that media import was not successful.

Platform: Platform Independent

Subsystem: Import Media Tool

Workaround: None

Bug ID: 17946

Description: The Windows 98-based boot disks can put the partition table in a bad state. After using the auto-partition option and rebooting the server, the boot disks fail while booting DOS (before getting to autoexec).

Platform: Windows

Subsystem: Provisioning

Error Message:

```
The configuration specified in your CONFIG.SYS file is
too large for memory. Remove some drivers and then try
again.

Type the name of the command interpreter.
```

Workaround: Follow these steps**:**

1. Boot the server from a DOS boot floppy that does not include network drivers.

2. Run fdisk from the floppy.

3. Remove all partitions.
4. Boot the server by using PXE boot.
5. At the PXE menu, select undi98 as the type of Opsware Build Agent to install on the server.

Bug ID: 17957

Description: My Jobs is not reporting when it encounters a problem in the reconcile step of OS provisioning.

For example, the OS definition used to install Solaris 5.9 on a server had a patch in it. A problem occurred when applying this patch (i.e. a user error), such that the reconcile part of provisioning the server reported "Completed with warnings". However, this was not reflected in the My Jobs table. Instead, the My Jobs table entry corresponding to the provisioning of this server has a status of "Completed" rather than "Completed with warnings" as expected.

Platform: Solaris 5.9

Subsystem: OS Provisioning

Workaround: Check the results of each reconcile to make sure there were no warnings when building and testing out a new profile.

Bug ID: 18017

Description: The Windows OS provisioning default timeout, which is 1 hour, is insufficient to install Windows 2003 on some servers.

Platform: Windows

Subsystem: OS Provisioning

Workaround: Set a custom attribute named "timeout" on the OS Definition and set it to the number of minutes you want, not to exceed four hours.

Bug ID: 19825

Description: Installation of the Operating System fails after the first reboot.

```
Error: Boot load failed.
The file just loaded does not appear to be executable.
```

This occurs if the OS media used for installation does not support the hardware architecture. An example would be using Solaris 8 12/03 hardware media that supports sun4u platforms only to build a sun4us server. The solution is to use appropriate OS media that supports the required hardware architecture.

```
Error: krtld: load_exec: fail to expand cpu/$CPU
```

This occurs if the OS media does not support the hardware CPU. The solution is to add required system patches that support the system CPU model using a build customization script that will install the patches in the post-Jumpstart phase.

```
Error: Cannot assemble drivers for root
```

This error occurs if disk adapter drivers for the root servers are not installed prior to the first reboot. The solution is to install the disk adapter drivers using a build customization script that will install the driver in the post-Jumpstart phase.

Platform: Any SunOS version

Subsystem: OS Provisioning

Bug ID: 20263

Description: On Dell PE650 servers, the OS Provisioning Subsystem can fail to boot the server. Anaconda fails to mount the directory /opt/OPSWboot/Opsware on the Opsware Boot Manager.

Platform: Linux

Subsystem: OS Provisioning

Workaround: Retry manually to mount the NFS location. The server will then be able to register with the Opsware System.

Patch Management Subsystem

Bug ID: 13336

Description: Java script error when uploading patches with two concurrent sessions.

Platform: Platform Independent

Subsystem: Upload Patch Wizard

Symptom: When uploading OS Service Pack in one window and initiating another patch upload for Application service pack using the Upload Patch Wizard in another window, a Javascript error, "wizardProgressPage is undefined" may appear.

Workaround: None

Bug ID: 13390

Description: Microsoft distinguishes Hotfixes that are the same just different due to platform or product version by changing the case of the letters in the filename. However, when a user downloads the Hotfix from the Microsoft website, the Hotfix is downloaded with all capital letters in the filename. When the Opsware System uploads with patch into the Patch Management Subsystem with all capital letters in the filename, the Opsware System cannot distinguish the platform or product version of the Hotfix.

Platform: Windows

Subsystem: Patch Management

Workaround: Upload the Hotfix as exactly named (with the correct case) into the Opsware System. The correct case for the filename can be determined by viewing the Hotfix in the Patches channel in Opsware Command Center

1. Select Software ► Patches in the navigation panel.
2. In the Patches page, select the Hotfix name to open the View Patch page.
3. In the field "Patch File:" (in the Patch Summary section), find the correct value for the filename.
4. Download the Hotfix from Microsoft and save as that exact filename,
5. Upload that file into Opsware.

Bug ID: 14137

Description: Sometimes, the Install Patch wizard fails to refresh and show progress. In fact, the installation completes normally.

Platform: Platform Independent

Subsystem: Install Patch Wizard

Symptom: The following scenario demonstrates this problem:

- Install a patch on two AIX servers.
- The status for one of the servers becomes stuck at 7%.
- When you go to My Jobs and look at the status for this device, it shows 49%.

Workaround: None

Bug ID: 14219

Description: "Patch Data last modified Date" does not coincide with user preferences time zone.

Platform: Platform Independent

Subsystem: Patches

Symptom: The following scenario is an example of this problem: You set a cron job to upload mssecure @ 9:00 PM PST. It ran successfully and updated several patches; however, the "Patch Data Last Modified" date is not displayed in the time zone that the user selected. In this case, it is set to PST, the time stamp is shown as "8/14/03 02:00:10" where it should be "8/14/03 09:00:10". Consequently, the user is misinformed of the exact time when changes were made.

The timestamp is logged in /var/lc/mm_wordbot/wordbot.err as shown below:

```
[14/Aug/2003 09:00:10 +0000] DEBUG "Updating Unit for:
'/packages/any/nt/5.2/iis4fixi.exe', unit_id: 639040001L" -- -
- ""
```

Workaround: None

Bug ID: 14390

Description: The gzip and gunzip utilities must be installed on Sun Solaris 8 and 9 servers. If these utilities are not installed, attempts to install patches that are delivered in the gzip format fail.

Platform: Sun Solaris 8 and 9 servers

Subsystem: Patch Management

Workaround: Install the gzip/gunzip utilities on all Sun Solaris 8 and 9 servers.

Bug ID: 15604

Description: Uninstall Patch Wizard may display patches that are not installed.

A patch that fails to install via the Install Patch Wizard will appear as an uninstallable patch in the Uninstall Patch Wizard. The server is attached to the software node for the patch, but the patch is not, in fact, installed. The Uninstall Patch Wizard will complete in this case and the software node for the patch will be detached from the server.

Platform: Independent

Subsystem: Uninstall Patch Wizard

Workaround: None

Bug ID: 15624

Description: Users should not attach Solaris patch nodes to servers if the patches are already installed. Solaris patches that are not installed by the Opsware System cannot be uninstalled by the Opsware System. If, however, a user attempts to use the Opsware System to install a patch that had already been installed on a server, the patch itself is not affected (i.e., not reinstalled), but the patch appears in the Uninstall Patch Wizard. The patch cannot be uninstalled even though uninstalling the patch appears to be an option in the Uninstall Patch Wizard.

Platform: Solaris

Symptom: Patches that are not installed on a server appear as an uninstallable option in the Install Patch Wizard.

Workaround: Detach the server from the patch node using server management.

Bug ID: 17941

Description: Error when deprecating a Solaris patch.

Platform: Solaris

Subsystem: Patch Management

Error Message:

```
Your changes were not made due to the following error:
Error updating Package: Unable to update package 108434-
10 due to the following error: OpswareError:
spin.genericDatabase [ module: truthdb.py, method:
raiseOracleError, line: 620, hostname:
gold5.goldsox.qa.opsware.com, timestamp: 02/Apr/2004
224451, msg: ORA-01461: can bind a LONG value only for
insert into a LONG column ]
```

Workaround: None

Reconcile

Bug ID: 14343

Description: When an APAR/fileset install fails, the error message is misleading because it is referenced by a Maintenance Level.

Platform: Platform Independent

Subsystem: Reconcile Backend

Symptom: When a fileset referenced by an ML and an APAR is uninstalled by uninstalling the APAR, the operation is a no-op. But the following message, displayed in the output window, may be misleading.

```
https://192.168.218.130:1018/way/checkSession.py?session_
id=61030001&$drew=1&go=Go !
was_not_removed [{'unique_name': 'IY41249', 'unit_type':
'APAR', 'messages':
['This package was not removed.
Probably because a prior package failed causing the
Uninstall Patch to abort.']}]
```

Workaround: None

Software Repository (Word)

Bug ID: 8557

Description: The Wordclient and Word user interface is accessible only from servers that are registered with the Opsware Model Repository (Truth).

Platform: AIX, Solaris, and Linux

Subsystem: Manage Packages

Workaround: Add the IP addresses to the Model Repository (Truth) for systems that are used to access the Word user interface or upload and download the packages with the Opsware Command Center packages channel or the Opsware Command Line Interface (OCLI).

Bug ID: 14274

Description: Software Replication can get caught in an infinite loop following a symlink. Users can select which directories to have the Software Repository Replicator replicate. If one of those directories has a symlink that involves a circular reference, such as a symlink that points back to its parent directory, the Software Package Repository gets caught in an infinite loop.

Platform: Independent

Subsystem: Software Repository Replicator

Workaround: When selecting which directories to have the Software Replicator replicate, be certain not to include any directories that have symlinks that point back to their parent directories.

Bug ID: 20128

Description: You cannot use the Opsware Command Center or the OCLI to download a Fujitsu Recommended Patch Cluster that was previously uploaded to the Opsware System. This happens because Fujitsu patch clusters are created with unique virtual names based on hardware type. The attempt fails with the following error:

```
wordbot.FileNotFile
```

Platform: Fujitsu Solaris

Subsystem: Software Repository

Workaround: The patch cluster file is stored on the Software Repository filesystem and can be retrieved by accessing the filesystem. The default location of the Software Repository Solaris patch cluster files is: /cust/word/<facility>/packages/any/SunOS/<release>/<filename>

Web Services Data Access Engine

Bug ID: 19796

Description: ZSI (Zolera SOAP Infrastructure) uses a float format in constructing a SOAP decimal value. Python clients of the Web Services API that use ZSI proxy module may run into cases where the ID of an object causes a failure when converted into a Java BigDecimal on the server side.

Platform: Platform Independent

Subsystem: Web Services Data Access Engine

Workaround: Python clients of the Web Services API using ZSI proxy module should use the patched stub available from Opsware Inc.

Miscellaneous

Bug ID: 10163

Description: Long-running Multimaster tools requests time out. The Opsware Command Center gives a proxy timeout error on long Multimaster tools requests. Some Multimaster operations take a long time, such as calculating the transaction differences on a large set of Command Engine results. After 10 minutes, the Opsware Command Center returns an error about the proxy not responding. It is possible that you will be unable to resolve Multimaster conflicts because of this problem. If this situation occurs, contact Opsware Technical Support for assistance.

Platform: Platform Independent

Subsystem: Multimaster

Error Message:

```
Proxy not responding
```

Symptom: Multimaster transactions time out after 10 minutes.

Workaround: None

Bug ID: 12001

Description: The servers running Opsware System components are not protected against reconcile operations that reboot the servers or against removing an Opsware node.

Workaround: Do not reconcile any servers on which Opsware core components are installed.

Bug ID: 15722

Description: 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 they 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.

Platform: Independent

Symptom: Components will start and appear to be up, but will not properly authenticate anyone who attempts to log into them.

Workaround: Restart the Command Engine after the Data Access Engine is up.

Bug ID: 17801

Description: A race condition occurs during Opsware installation on a slow machine.

Platform: Linux, Solaris

Subsystem: Installer

Workaround: Verify that the Data Access Engine has started up and is listening on port 1004. Then, re-run the installer, and again select Data Access Engine from the components menu.

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.