OPSWARE INC
Automating IT™

Opsware® System 4.5

Release Notes

Copyright © 2000-2004 Opsware Inc.

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

Opsware, Opsware Command Center, Model Repository, Data Access Engine, Web
Services Data Access Engine, Software Repository, Command Engine, Opsware
Agent, Multimaster Replication Engine, and Code Deployment & Rollback are
trademarks and service marks of Opsware Inc. All other marks mentioned in this
document are the property of their respective owners.

The Opsware System is protected by US and international copyrights and patents
pending.

Table of Contents

Introduction to Opsware System 4.5

Opsware System 4.5 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.

Support for DVD-based installation has been added.

Also new with Opsware System 4.5 is support for an all-Linux core. Three new managed server platforms have also been added:

- Solaris 2.8 and 2.9 for Fujitsu PrimePower

- SuSE Linux Standard Edition 8.0.

Opsware System 4.5 includes the following new features:

- Agent Reachability Communication Test

- Agent Uninstaller

- Opsware Extension for Server Recertification

- New Public Database View

- 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

What's New In Opsware System 4.5

Agent Reachability Communication Test

The new Agent Reachability Communication Test in Opsware System 4.5 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 retrieves 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 Mismatch (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 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" 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 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 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 Servers" in *Opsware System 4.5 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 User's Guide*, Chapter 2 for more information.

- **Creating Communication Test DCI reports** – Allows you to create a printable report of the Communication Test result by using the DCI report tool. See DCI Online Help for information about how to create a DCI Communication Test report.

- **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 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 User's Guide*, Chapter 2 for more information.

Agent Uninstaller

New in Opsware System 4.5 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, 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 Server 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 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.

Opsware 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 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.

New Public Database View

The Opsware System makes the public database views available so that you can create custom reports with either the Opsware System Data Center Intelligence module, or your own reporting system. A list of public database views is available in Appendix A of the *Opsware System 4.0 Data Center Intelligence Administrator's Guide*, available on the Opsware System download site.

In addition to the public database views shown in that document, a new one has been added called security_users_vw, which shows a list of users in the database and the date of their most recent login. This view has the following fields.

Field Name	Value
USER_ID	NOT NULL NUMBER

USERNAME	NOT NULL VARCHAR2(35)
MOST_RECENT_LOGIN	DATE

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.

User Interface Improvements

A number of improvements were made to the Opsware System User Interface.

Terminology Change – Server Cart Changed to My Servers

In the Opsware Command Center, the term Server Cart has changed to My Servers. This change appears in the navigation panel and in the Server menu in the Managed Servers feature. Other than the terminology change, the My Servers feature functions the same as it has previously.

See the *Opsware System 4.5 User's Guide*, Chapter 2 for information about how to use this feature.

Reorganization of the Managed Servers Area

In the Managed Servers list, the tabs and menu organization have changed.
Specifically, the Status, Software, and Hardware tabs are replaced with a new View
menu. The View menu includes a new option to view servers by how the Opsware
Agents running on those servers are communicating with the Opsware System.

Additionally, the choices in the menu are reorganized. In Opsware System 4.5, the
menu choices for Operating System, Patch, and Application are combined under the
new Software menu.

Managed Servers UI in Opsware System 4.0, 4.01, and 4.02
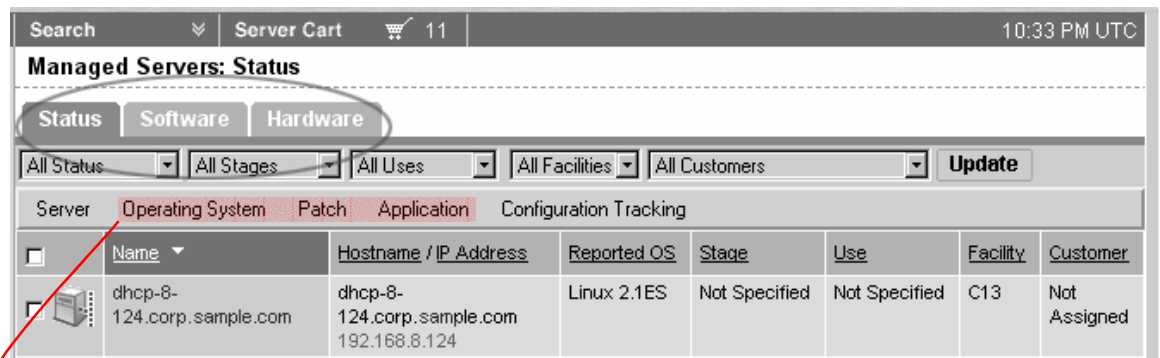
Managed Servers UI in Opsware System 4.5
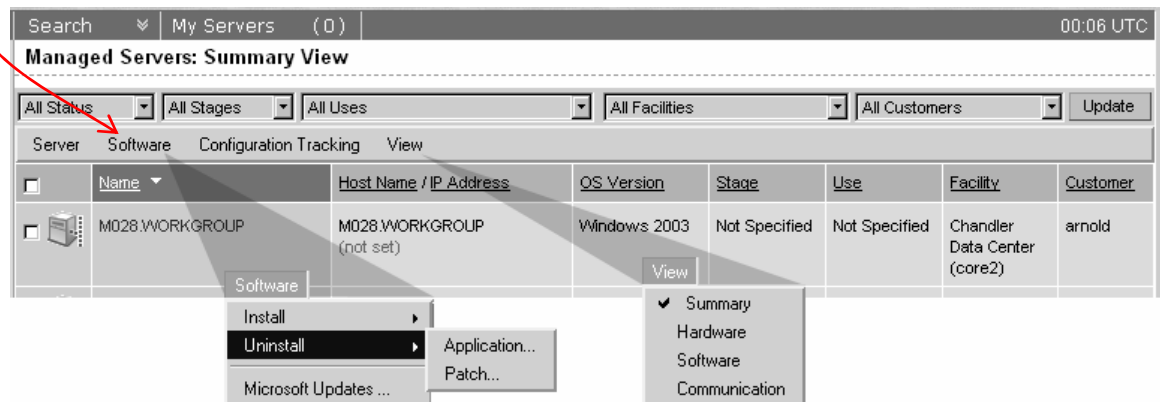
Hardware Registration Reliability and Opsware Agent Reporting

In Opsware System 4.5, hardware registration does *not* fail when the Opsware Agent encounters problems while gathering hardware inventory or when the Opsware System encounters problems processing incorrectly formatted or flawed hardware data that the Opsware Agent presented.

When a value cannot be determined for an attribute (for example, data is missing or non-existent for interfaces, memory, disks, and so forth), the Opsware Command Center displays *(not set)* in that hardware attribute field. DCI reports also display *not set* for the missing attribute. The hardware inventory proceeds past the missing attribute to obtain the rest of the data on the server. The existing value for the missing attribute remains in the Model Repository until the Opsware Agent next performs a full hardware registration and obtains that value.

The screen shot on the following page shows the Reported Information Section of a Server Properties Page.

⚠ REPORTED INFORMATION (as of 07/27/04 04:53:18) [+]	
Reporting:	Reporting error
Agent Version:	25.0.0.22
Hostname:	snv1.corp.sample.com
Reported OS:	Linux 7.2
MAC Address:	00:01:03:1F:B6:7C
Serial Number:	*(not set)* Serial Number Reporting Error
Chassis ID:	00:01:03:1F:B6:7C
Manufacturer:	DELL COMPUTER CORPORATION
Model:	XPS-Z
CPUs:	**Vendor** **Model** **Speed** **Cache Size** GENUINEINTEL Pentium III (Coppermine) 730 MHz 256 KB
Memory:	**Type** **Capacity** RAM 375.23 MB SWAP 509.87 MB
Storage:	**Drive** **Media** **Capacity** **Bus Type** **Model** hda DISK 19.01 GB IDE QUANTUM FIREBALLP LM20.4 hdc CDROM -- IDE Lite-On LTN483S 48x Max
Network:	See the Network tab

Serial number correctly
reported by the Opsware Agent ——▶ **Serial Number:** 6J09FCX290DN

In a server's properties page, the Reporting field indicates the status of the Opsware Agent's reporting capability, and tells you whether or not the Opsware Agent is reporting hardware inventory regularly and successfully. The four possible reporting states for the Opsware Agent are:

OK: Opsware Agent is reporting properly.

Registration in progress: Opsware Agent is currently registering server hardware information. This is reported within the first hour of an agent's first deployment on a server.

Reporting error: Opsware Agent encountered an error while trying to report hardware information.

Last reported days ago: This state indicates when the Opsware Agent last reported.

See "Opsware Agent on Managed Servers Overview" in Chapter 2 in the *Opsware System 4.5 User's Guide* for more information about viewing Opsware Agent reporting information for managed servers.

If the Opsware Agent experiences an error in reporting, or has not reported within 24 hours, you can run a Communication Test to troubleshoot the problem. See "Agent Reachability Communication Test" in Chapter 2 in the *Opsware System 4.5 User's Guide* for more information.

When an Opsware Agent is unable to report a full hardware inventory, you can click the plus sign (+) in the Reported Information heading to retrieve diagnostic data from the Opsware Agent. See the screen shot on the following page for an example.
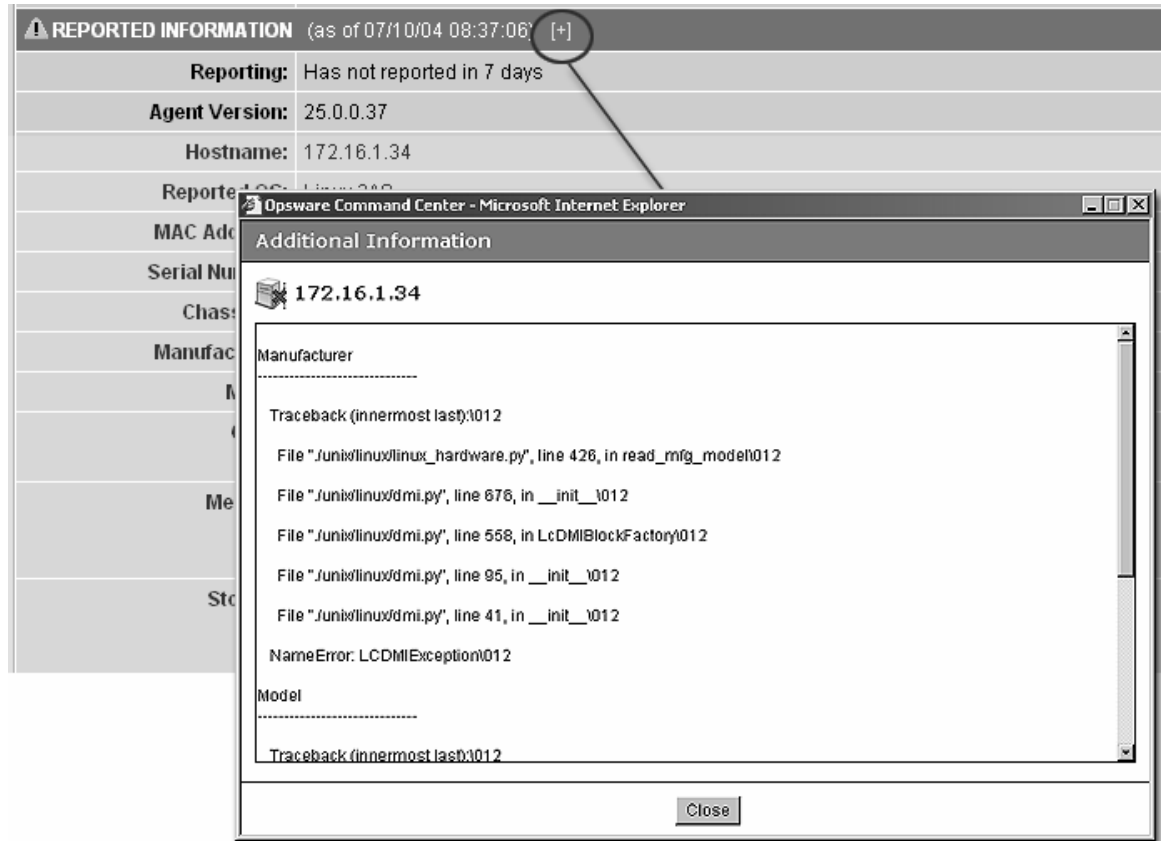
Hardware and Software Registration Efficiency

Hardware and software registrations are actions that are performed frequently during common operations such as Reconcile. In Opsware System 4.5, the process for hardware and software registration has changed to increase system efficiency and decrease the processing load on the managed servers.

On installation or upgrade, the Opsware Agent performs a minimal hardware and software registration asynchronously. Subsequent full registrations also occur asynchronously.

In Opsware System 4.5, the Opsware Agent maintains a local cache of hardware and software information. When the content of the cache is up-to-date, the Opsware Agent

reports to the Opsware System that the hardware and software inventory has not changed and does not re-send the entire inventory.

Additionally, to reduce the load placed on a managed server, Opsware System 4.5 lowers the runtime priority of the OS commands (such as, showrev, rpm,and so forth) that the Opsware Agent uses to gather data about the system.

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, 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.

Special Note About Japanese Versions

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

- When downloading ms 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 Sun operating 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.

Documentation Errata

Updates to the Opsware System 4.5 Administration Guide

The following topics in the *Opsware System 4.5 Administration Guide* are updated with new information.

Adding Users to a User Group

Replace the following figure with the figure in these release notes.

Figure: Edit Group User Assignment Page

Assigning Opsware System Permissions to a User Group

After you define a user group, you assign Opsware System permissions that determine the features and functionality that user group members have access to in the Opsware Command Center when they log in with their user names and passwords. When users log in, only those features or areas of functionality that they have access to through their membership in user groups appears in the Opsware Command Center navigation panel.

Perform the following steps to assign Opsware System Permissions to a User Group:

1. From the navigation panel, click Users & Groups under Administration. The Users & Groups: View Users page appears.

2. Click the Groups tab. The Users & Groups: View Groups page appears, which shows a list of all groups.

3. Click the hyperlinked name that corresponds to the user group you want to edit.

4. Click the Other tab.

5. Select the General permissions items for the group by clicking the check box next to the permissions you want to grant, as shown in the figure below.

Figure: General Permissions Section of Opsware Permissions Page

General Permissions	
☑	Deactivate
☑	Edit Shared Scripts
☑	Run My Scripts as Root

6. Select the Locking permissions for the group by clicking the check box next to the permissions you want to grant, as shown in the figure below.

Figure: Locking Permissions Section of Opsware Permissions Page

Locking Permissions	
☑	Application Servers
☑	Other Applications
☑	Database Servers
☑	OS Extras
☑	Service Levels
☑	System Utilities
☑	Web Servers

7. Click the Save button. A confirmation message appears confirming your permission change. Click Continue to return to the Permissions page.

8. Click the Customer tab.

9. Select the Customer permissions for the group by clicking the check box next to the permissions you want to grant and select Read or Read & Write access for that customer, as shown in the figure below.

Figure 2-19: Customer Permissions Section of Opsware Permissions Page

10. Click the Save button. A confirmation message appears confirming your permission change. Click Continue to return the Permissions page.

11. Click the Facilities tab.

12. Select the Facility permissions for the group by clicking the check box next to the permissions you want to grant and select Read or Read & Write access for that facility, as shown in the following figure.

Figure: Facility Permissions Section of Opsware Permissions Page

13. Click the Save button. A confirmation message appears confirming your
    permission change. Click Continue to return the Permissions page.

General Machine Health

The Opsware System Diagnosis tool *no* longer includes an option to run an Opsware
System Diagnosis test on managed servers to test the status of the Opsware Agents
running on those servers.

The topic "General Machine Health" in Chapter 3 of the Opsware System 4.5
Administration Guide has been replaced by the topic "Agent Reachability
Communication Test" (and the subtopics within this section) in Chapter 2 in the
Opsware System 4.5 User's Guide.

Running a System Diagnosis of Managed Servers

The Opsware System Diagnosis tool *no* longer includes an option to run an Opsware System Diagnosis test on managed servers to test the status of the Opsware Agents running on those servers.

The topic "Running a System Diagnosis of Managed Servers" in Chapter 3 of the *Opsware System 4.5 Administration Guide* has been replaced by the topics "Running a Communication Test on an Individual Server" and "Running a Communication Test on Multiple Servers" in Chapter 2 in the *Opsware System 4.5 User's Guide*.

Updates to the Opsware System 4.5 User's Guide

In the printed version of the *Opsware System 4.5 User's Guide*, these release notes update the content in the following ways:

- The term "Communications Test" (which is plural) is updated by term "Communication Test" (which is singular).

- The system clock in the Opsware Command Center top navigation displays the time in the format *HH*:*MM TZ* (where TZ is the time zone) and 24-hour format.

- The topic "Adding Custom Attributes to an OS Definition" in Chapter 3 is updated by the new topic in these release notes.

- The topic "Uploading a Package" in Chapter 5 is updated by the new topic in these release notes. The new topic in these release notes indicate how you can specify a package encoding scheme when uploading a package.

- In Appendix D: "Communication Test Troubleshooting," the Communication Test result names are updated.

Adding Custom Attributes to an OS Definition

Perform the following steps to add custom attributes to an OS definition:

1. Click Software ► Operating Systems from the navigation panel. The Operating Systems page appears.

2. Click the display name of the OS you want to edit. The Edit Operating System page appears.

3. Click the Custom Attributes tab. The list of custom attributes specified for the OS definition appears, as shown in the figure below.

Figure: Custom Attributes Tab for an OS Definition in the Opsware Command Center
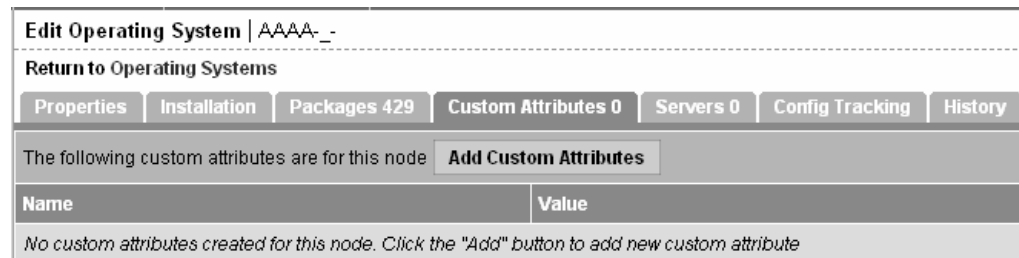
Note   *If the OS Definition contains custom attributes, the Edit Custom Attributes button appears in the page. Click the Edit Custom Attributes button to add new attributes and edit existing ones.*

4. Click the Add Custom Attribute button. A page appears in which you can enter the names and values for custom attributes.

5. Enter a name and a value for the custom attribute.

6. Click the Save button. The list of custom attributes set for the OS definition reappears. The new custom attribute is added to the list.

Uploading a Package

Each operating system supported by the Opsware System supports certain package types. See "Supported Operating Systems and Package Types" in Chapter 3 for more information.

If a package that is being uploaded already exists in the Software Repository, the Opsware System overwrites the package. See "Overwriting a Package" in Chapter 3 for more information.

If you upload Solaris patch clusters that contain patches that already exist in the Software Repository, the patches are overwritten. However, the Opsware System preserves any reboot options or flags set for the patches in the Opsware Command Center.

If an update fileset is part of many different APARs, the Opsware System can take a long time to upload the LPP that contains it, because it must create a large number of APARs in the list of packages. The package upload can appear to time-out in the Opsware Command Center. However, the Opsware System continues to upload the package.

When you upload a Windows MSI package, the information you enter about the package must match the internal data (ProductName and ProductVersion) stored in the file or the Opsware System reports errors when the package is installed on servers.

To obtain the ProductName and ProductVersion from an MSI package, use the Orca tool from Microsoft Corporation. You can download this tool as part of the MSI software developers' kit (SDK) v1.2. See "MSI Package Metadata" in Chapter 3 for information on how to obtain and use Orca.

Perform the following steps to upload a package:

1. From the navigation panel, click Packages under Software. The Packages: Browse Packages page appears.

2. Click the Upload tab. The Packages: Upload Package page appears, as shown in the figure below.

Figure: Upload Package, Specify Basic Properties Page

3. Specify the operating system and customer for which the package is to be used:

    Customer – specifies the customer for which packages will be used. Options for customer selections are those that your Opsware administrator defines by using the Opsware Administration channel.

    When you upload any patch, Windows utility, or Microsoft Patch database, the file is automatically associated with Customer Independent regardless of the customer you select from the drop-down list. HP-UX depots that contain both products and patch products cannot be uploaded to a specific customer. They can only be uploaded to Customer Independent.

    Operating System – specifies the operating system for which the package is to be used. You can select from specific operating systems that your Opsware administrator set up.

When you select a Windows utility or Microsoft database, the operating system is automatically set to Windows 2000.

Type – specifies the package type for the operating system selected. Certain package types, for example, patches or Windows utilities, force the customer to be Customer Independent.

The Opsware System verifies that RPMs, Solaris patch clusters, AIX LPPs, Solaris packages, and HP-UX depots uploaded are the correct package type.

4. Click the Next button. If you select Windows MSI or OS Service Pack as the package type, a second form appears that prompts you to enter additional metadata for the package, as shown in the figure below.

Figure: Upload Package, Specify Extended Properties Page

5. If necessary, enter additional required information for the package and click the Next button. A page appears that prompts you to specify the location of the package file.

    a.   In the **Local Path to Package** field, enter the name and directory location of the package that you want to upload or click the Browse button to locate and select the package to upload.

    b.   In the **Encoding of metainformation in package** field, select the encoding scheme to be used by the package.

        You need to specify an encoding scheme so that the Opsware System can extract the meta-data contained in the package and correctly display the information in non-ASCII characters in the Opsware Command Center (for example, in the Package Properties pages).

6.   Click the Upload button.

If a package (excluding AIX LPPs, HP-UX depots, and Solaris packages) with the same name already exists in the Software Repository for the same customer and operating system, the Opsware Command Center overwrites the existing file after it prompts you to confirm your choice. See "Overwriting a Package" on page 294 for more information.

After you upload the package, the Opsware Command Center displays a page in which you can enter additional package file property information.

If you are uploading a Solaris package, you can upload a response file for each of its instances by editing the response file's package properties for those instances.

See "Editing Package Properties" in Chapter 3 in the *Opsware System 4.5 User's Guide* for a description of additional properties that you can specify and the steps to upload a response file for a Solaris package instance.

Creating a Script

How to Create or Upload a Script

Use the following procedure to create or upload a My Script or Shared Script:

1. From the navigation panel, select Scripts under Software.

   On the Scripts page, there are two tabs – My Scripts and Shared Scripts.

2. To create or upload a My Script, click the My Scripts tab, then click New Script. The

   New Script page appears.

3. To create or upload a Shared Script, click the Shared Scripts tab, and then click New Script. The New Script page appears, as shown in the figure below.

Figure: The New Script Page

Scripts: New Script

Return to Scripts

Properties

Name:	
Type:	Unix Shell
Shared:	○ Yes ● No
Changes Server?	○ No ● Yes

Script Contents

● **Enter Script Contents:**

○ **Upload Script:**

Encoding of script: ASCII

Local Path to Script: [Browse...]

Usage Notes

Usage Notes are required

[Save] [Cancel]

4.   On the Scripts: New Script page, enter the following data under Properties:

- Enter the **name** of the script. The name must be a unique shared-use or personal-use name.

- Select the **script type**: Unix shell, Windows .BAT or Windows VBScript.

- If you are creating a Shared Script, select Yes next to "Shared." If you are creating a My Script, select No.

- In the **Changes Server** field, select No if the script does not modify the server, and Yes if it does. If Yes is selected, locked servers cannot be selected to run that script.

5. Under **Script Contents**, enter or upload a script by performing one of the following tasks:

- To upload a script, click Upload Script. In the Local Path to Script box, either manually enter the path to the script, or click Browse to locate the script.

*NOTE   When you upload a script, you **must** select an encoding scheme for the script from the list so that the Opsware System can convert the bytes inside the script into UTF-8 format by using the encoding scheme with which the script was created.*

- To create a script, click Enter Script Contents and manually enter the script in the text box.

NOTE   The scripts editor does not recognize tabs and its functionality is browser-dependent.

6. In the Usage Notes section of the page, enter script details or other descriptive information.

7. Click Save to store the script. The script is saved in the Model Repository.

The Scripts page appears and confirms that the script is now stored. The script is included in the list of available Shared Scripts or My Scripts.

Encoding Schemes for Package Metadata and Scripts

In Opsware System 4.5, you can specify encoding schemes for package metadata and scripts in the following ways:

- Specify the encoding scheme for package metadata when uploading packages in the Opsware Command Center (in the Packages channel and Software Install Wizard) or by using the Opsware Command Line Interface (OCLI).

  When specified, the Opsware Command Center correctly displays in non-ASCII any package meta-data, description fields, and error and status message returned by the operating system of the managed servers.

- Specify the encoding scheme for scripts when uploading them in the Opsware Command Center (in the Run Distributed Script Wizard and Scripts channel).

  A user must specify an encoding scheme for an uploaded script so that the Opsware System can convert the bytes inside the script into UTF-8 format by using the encoding scheme with which the script was created.

  After scripts run, users can download a zip file containing the results encoded in UTF-8 format.

  For example, on Unix operating systems, you can use iconv (the code set conversion function) to interpret the downloaded results of the script execution.

The Opsware Command Center includes the following selections for encoding schemes:

- ASCII

- BIG5

- BIG5-HKSCS

- CP850, CP862, CP866, CP874, CP932, CP949, CP950, CP1133, CP1250, CP1251, CP1252, CP1253, CP1254, CP1255, CP1257, CP1258, CP1266

- EUC-CN, EUC-JP, EUC-KR, EUC-TW

- GB18030, GBK

- GEORGIAN-ACADEMY

- GEORGIA

- N-PS

- HZ

- ISO-2020-CN, ISO-2020-CN-EXT, ISO-20202-KR, ISO-2022-JP, ISO-8859-1, ISO-8859-2, ISO-8859-3, ISO-8859-4, ISO-8859-5, ISO-8859-6, ISO-8859-7, ISO-8859-8, ISO-8859-9, ISO-8859-10, ISO-8859-13, ISO-8859-14, ISO-8859-15, ISO-8859-16

- JOHAB

- KOI8-R, KOI8-RU, KOI8-T, KOI8-U

- MULELAO-1

- SHIFT_JIS

- TCVN

- TIS-620

- UCS-2, UCS-4

- UTF-8

- VISCII

Specifying an Encoding Scheme in the Opsware Command Line Interface (OCLI)

In Opsware System 4.0.1, Japanese Edition, the Opsware Command Line Interface (OCLI) was updated with new arguments to allow you to specify an encoding scheme when uploading and downloading packages and for the customer display name.

See *Opsware System 4.0 User's Guide*, Appendix A: "Opsware Command Line Interface" for information about using the OCLI and the supported arguments.

New Arguments for the oupload Command

NOTE   *You only need to enter these arguments when you want to override the default*
settings in the LANG environment variable in your shell.

Argument	Value	Description
--filename-encoding (-e)	String	Specifies the character set of the file name. When specifying non-ASCII characters in the value for the --customer argument, include the –e argument on the command line to tell the Opsware System which character set to use when communicating with the Opsware System Model Repository database.
--metainfo-encoding (-E)	String	Specifies the character set of the meta-information in the package.

New Argument for the odownload Command

NOTE   *You only need to enter this argument when you want to override the default settings in*
the LANG environment variable in your shell.

Argument	Value	Description
--filename-encoding (-e)	String	Specifies the character set encoding in which to save the file name.

Communication Test Result Names

In Appendix D: Communication Test Troubleshooting, the Communication Test result names are updated in the following ways:

Result Name in Printed Guide	Updated Result Name
AGT – Test Passed	Command Engine to Agent (AGT) - OK
AGT – Untested	Command Engine to Agent (AGT) - Untested
AGT – Unexpected Error	Command Engine to Agent (AGT) - Unexpected error
AGT – Connection Refused	Command Engine to Agent (AGT) - Connection refused
AGT – Connection Timeout	Command Engine to Agent (AGT) - Connection timeout
AGT – Request Timeout	Command Engine to Agent (AGT) - Request timeout
AGT – Server Not Registered with the Command Engine	Command Engine to Agent (AGT) - Server never registered
AGT – Realm is Unreachable	Command Engine to Agent (AGT) - Realm is unreachable
AGT – Tunnel Setup Error	Command Engine to Agent (AGT) - Tunnel setup error

Result Name in Printed Guide	Updated Result Name
AGT – Gateway Denied Access	Command Engine to Agent (AGT) - Gateway denied access
AGT – Internal Gateway Error	Command Engine to Agent (AGT) - Internal gateway error
AGT – Gateway Couldn't Connect to Server	Command Engine to Agent (AGT) - Gateway could not connect to server
AGT – Gateway Timeout	Command Engine to Agent (AGT) - Gateway timeout
CRP – Test Passed	Crypto Match (CRP) - OK
CRP – Untested	Crypto Match (CRP) - Untested
CRP – Unexpected Error	Crypto Match (CRP) - Unexpected error
CRP – Certificate Mismatch	Crypto Match (CRP) - Agent certificate mismatch
CRP – SSL Negotiation Failure	Crypto Match (CRP) - SSL negotiation failure
CE – Test Passed	Agent to Command Engine (CE) - OK
CE – Untested	Agent to Command Engine (CE) - Untested
CE – Unexpected Error	Agent to Command Engine (CE) - Unexpected error

Result Name in Printed Guide	Updated Result Name
CE – Connection Refused	Agent to Command Engine (CE) - Connection refused
CE – Connection Timeout	Agent to Command Engine (CE) - Connection timeout
CE – Command Engine Name Does Not Resolve	Agent to Command Engine (CE) - DNS does not resolve
CE – Old Agent Version	Agent to Command Engine (CE) - Old agent version
CE – Realm is Unreachable	Agent to Command Engine (CE) - Realm is unreachable
CE – No Gateway Defined	Agent to Command Engine (CE) - No gateway defined
CE – Tunnel Setup Error	Agent to Command Engine (CE) - Tunnel setup error
CE – Gateway Denied Access	Agent to Command Engine (CE) - Gateway denied access
CE – Name Resolution Error On Gateway	Agent to Command Engine (CE) - Gateway name resolution error
CE – Internal Gateway Error	Agent to Command Engine (CE) - Internal gateway error
CE – Gateway Couldn't Connect to Server	Agent to Command Engine (CE) - Gateway could not connect to server

Result Name in Printed Guide	Updated Result Name
CE – Gateway Timeout	Agent to Command Engine (CE) - Gateway timeout
CE – No Callback from Agent	Agent to Command Engine (CE) - No callback from agent
DAE – Test Passed	Agent to Data Access Engine (DAE) - OK
DAE – Untested	Agent to Data Access Engine (DAE) - Untested
DAE – Unexpected Error	Agent to Data Access Engine (DAE) - Unexpected error
DAE – Connection Refused	Agent to Data Access Engine (DAE) - Connection refused
DAE – Connection Timeout	Agent to Data Access Engine (DAE) - Connection timeout
DAE – Data Access Engine Name Does Not Resolve	Agent to Data Access Engine (DAE) - DNS does not resolve
DAE – Old Agent Version	Agent to Data Access Engine (DAE) - Old agent version
DAE – Realm is Unreachable	Agent to Data Access Engine (DAE) - Realm is unreachable
DAE – No Gateway Defined	Agent to Data Access Engine (DAE) - No gateway defined

Result Name in Printed Guide	Updated Result Name
DAE – Tunnel Setup Error	Agent to Data Access Engine (DAE) - Tunnel setup error
DAE – Gateway Denied Access	Agent to Data Access Engine (DAE) - Gateway denied access
DAE – Name Resolution Error On Gateway	Agent to Data Access Engine (DAE) - Gateway name resolution error
DAE – Internal Gateway Error	Agent to Data Access Engine (DAE) - Internal gateway error
DAE – Gateway Couldn't Connect to Server	Agent to Data Access Engine (DAE) - Gateway could not connect to server
DAE – Gateway Timeout	Agent to Data Access Engine (DAE) - Gateway timeout
SWR – Test Passed	Agent to Software Repository (SWR) - OK
SWR – Untested	Agent to Software Repository (SWR) - Untested
SWR – Unexpected Error	Agent to Software Repository (SWR) - Unexpected error
SWR – Connection Refused	Agent to Software Repository (SWR) - Connection refused
SWR – Connection Timeout	Agent to Software Repository (SWR) - Connection timeout

Result Name in Printed Guide	Updated Result Name
SWR – Software Repository Name Does Not Resolve	Agent to Software Repository (SWR) - DNS does not resolve
SWR – Old Agent Version	Agent to Software Repository (SWR) - Old agent version
SWR - Server Identification Error	Agent to Software Repository (SWR) - Server identification error
SWR – Realm is Unreachable	Agent to Software Repository (SWR) - Realm is unreachable
SWR – No Gateway Defined	Agent to Software Repository (SWR) - No gateway defined
SWR – Tunnel Setup Error	Agent to Software Repository (SWR) - Tunnel setup error
SWR – Gateway Denied Access	Agent to Software Repository (SWR) - Gateway denied access
SWR – Name Resolution Error On Gateway	Agent to Software Repository (SWR) - Gateway name resolution error
SWR – Internal Gateway Error	Agent to Software Repository (SWR) - Internal gateway error
SWR – Gateway Couldn't Connect to Server	Agent to Software Repository (SWR) - Gateway could not connect to server
SWR – Gateway Timeout	Agent to Software Repository (SWR) - Gateway timeout

Result Name in Printed Guide	Updated Result Name
MID – Test Passed	Machine ID Match (MID) - OK
MID – Untested	Machine ID Match (MID) - Untested
MID – Unexpected Error	Machine ID Match (MID) - Unexpected error
MID – Mismatch	Machine ID Match (MID) - MID mismatch

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 4.5 supports. For complete information on package types and file types, see Chapter 5, Package Management, in the *Opsware System 4.5 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)	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, Workstation 3.0)	RPM	.rpm
SuSE Linux (Enterprise Server 8.0, Standard Server 8.0	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 (4.33, 5.1, 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, 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

These are the browsers that Opsware System 4.5 supports.

Browser	Windows 2000	Windows 2003	Windows XP	Linux 6.2+	Sunos 5.6+	Apple os x
Microsoft Internet Explorer 5.5	X					
Microsoft Internet Explorer 6.0	X	X	X			
Mozilla 1.6		X	X	X	X	X

Supported Core Platforms

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

The Data Center Intelligence Server runs on Windows 2000.

NOTE: Running the Opsware System core on SunOS 5.9 is not supported in this release.

Supported Installations

The Opsware System 4.5 release supports the following installations:

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

- First time, from-scratch installation of multimaster cores

- Upgrade from Opsware System 4.0.2 to Opsware System 4.5. Refer to the *Opsware System 4.5 Upgrade Guide* for more information.

Documentation

This release comes with the following documentation:

- *Opsware System 4.5 Release Notes*
- *Opsware System 4.5 Upgrade Guide*
- *Opsware System 4.5 Installation Guide*
- *Opsware System 4.5 User's Guide*
- *Opsware System 4.5 Administration Guide*
- *Opsware System 4.5 Web Services API*
- *Version 1.1 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.

Agent Compatibility

Refer to the following table for information about the compatibility of new functions included in Opsware System 4.5 with Opsware Agents from earlier releases.

4.5 Feature	4.0.1 and Earlier Agents
Agent Reachability Communications Test	This feature is only functional with Opsware System 4.5 cores and agents.
Agent Uninstaller	This feature is only functional with Opsware System 4.5 cores and agents.
Fujitus Solaris 2.8 and 2.9 SuSE Linux Standard Edition 8.0	Support for these platforms is new in Opsware System 4.5, so no previous agent compatibility.

What's Fixed in Opsware System 4.5

The following bugs that have a severity level of Critical or Major that are fixed in Opsware System 4.5.

Configuration Tracking Subsystem

Bug ID: 15677, 15679 and 15681

Description: Cannot restore backed-up Windows Registry keys or COM+ objects, or an IIS Metabase after a migration to Opsware System 4.0.1. If a managed server with a backed up Windows Registry key is running an older Opsware Agent, the Windows Registry key cannot be restored after migrating to Opsware System 4.0.1.

Platform: Windows

Subsystem: Configuration Tracking

Error Message:

```
Name: Failed to Perform Restore
Description: An error occurred restoring some
file(s)/target(s) while attempting to restore data to the
server. All targets not listed were successfully restored.
```

Symptom: Windows Registry key restoration fails.

Resolution: This was a problem in older releases, but more recent engineering developments render this problem obsolete.

Bug ID: 18091

Description: File not found error when attempting to download Configuration Tracking backup file in a multi-word environment.

Platform: Platform Independent

Subsystem: Configuration Tracking

Error Message: Error Summary

```
Name: File Not Found
Description: The requested file cannot be found in the
Package Repository.
Error Details
Error ID: 17720318
Error Name: File Not Found
Time: 12/Apr/2004 235003
Hostname: gold5.goldsox.qa.opsware.com
File: /acsbar/0/210318L/410318L/manifest.xml
Exception Info: OpswareError: wordbot.FileNotFound [
module: server.py, method: getWordStoreFileInfo, line:
1402, hostname: gold5.goldsox.qa.opsware.com, timestamp:
12/Apr/2004 235003, file:
/acsbar/0/210318L/410318L/manifest.xml ]
```

Resolution: The Software Repository now checks satellite data centers to retrieve configstore backup files.

Bug ID: 18128

Description: When selecting multiple servers, clicking the link for a Configuration Tracking Policy entry in the View Backup History page displays policy entries for other servers.

Platform: Platform Independent

Subsystem: Configuration Tracking

Resolution: This has been fixed so that when the "Tracking Policy" page for a device is shown (when accessing it through the "View Backup History" page for multiple servers), only the policies for that selected server are shown, instead of for all of the previously-selected servers.

Data Center Intelligence (DCI)

Bug ID: 18077

Description: There have been some problems with connections from DCI to the Model Repository leaving open INACTIVE sessions.

Platform: Platform Independent

Subsystem: Model Repository (Truth)

Resolution: A profile limiting idle time to 60 minutes has been created for the opsware_public_views user. This means that the opsware_admin_user needs three additional privileges: CREATE PROFILE, ALTER PROFILE, and DROP PROFILE.

Network Configuration

Bug ID: 17784

Description: Attempting a network configuration update on HP-UX failed.

Platform: HP-UX 11.11

Subsystem: Network Configuration

Error Message:

```
"New configuration did not stick", with the following
error details:
Job ID:  1620318
Status: FAILURE
Errors
Error Summary
Name:       New configuration did not stick
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:  3460318
Time:        03/25/04 19:26:36
Hostname:
m026core.cust.custqa11.com
Reverted configurations:
server default_gw
Unexpected changes:
server system_name
server dns_search_domains
```

Resolution: This was a symptom of bug 17669 (gateway information not reported). Since the gateway was reported as None, it didn't match what it was supposed to be changed to (and was correctly changed to). Now that the agent is reporting the gateway, this bug is no longer a problem.

Bug ID: 17951

Description: Network configuration does not show disabled NICs on AIX.

Platform: AIX

Subsystem: Network Configuration

Resolution: Fixed an agent bug which caused disabled network interfaces to go unreported

Opsware Agent (Cogbot)

Bug ID: 17757

Description: Reinstalling an Opsware Agent on a server fails due to issues with the cryptographic material and the need to re-cert the Opsware Agent. When reinstalling an Opsware Agent on a server, the following actions occur:

8.   A bootstrap certificate is used.

9.   The Opsware Agent on the server registers its hardware with the Opsware core before it requests new cryptographic material from the Opsware core.

10. The Opsware Agent requests new cryptographic material from the Opsware core.

Step 2 fails because of the equivalence test in the code for the two values for cert_subject_cn.

Platform: Platform Independent

Subsystem: Data Access Engine

Resolution: The Data Access Engine was modified so that it never checks the cert_subject_cn in the cert being provided by the Agent.

Bug ID: 18250

Description: Upgrading an agent on an HP-UX 10.20 server fails.

This is an infrequent error, and has not been reproduced.

Platform: HP-UX 10.20

Subsystem: Opsware Agent

Error Message:

```
root@gold4 bin]# ./opsh_agent review 51860318
Session 51860318L
Device ID   Name/IP address  Version Status  Reason
70318L      m063-hpux.cust.custqa6.com
FAILURE Opsware Agent installer did not shut down the
incumbent agent. Please retry the upgrade operation.
Session 51860318L completed.
From the Way session:
Thu Apr 22 21:41:59 EDT 2004
[INFO] Log started.
[ERROR] Unsupported system type : 'sh: uname:  not
found.'.
[INFO] Log ended.
```

Resolution: The Agent Installer has been modified to use an explicit path for uname.

Opsware Command Center

Bug ID: 13037

Description: Navigation of the Add function in the Software > Applications channel is confusing.

Platform: Platform Independent

Subsystem:

Resolution: Navigation has not changed, but once a user clicks Add, Edit, Server tab, History tab, and so forth, the navigation buttons will go away.

Bug ID: 15917

Description: Attempting to view the contents of a zip package that contains spaces in the filename results in an error message.

Platform: All Windows

Error Message:

```
There was an error retrieving the contents of this
package.
Error details:
Name: Error occurred while trying to query the package
for a list of files that it contains
Description: null
Error ID: 17550104
```

Resolution: The code that inspects the contents of a zip file has been updated to work with zip files with spaces in their filenames, and the Opsware Command Center is now able to display all such files.

OS Provisioning Subsystem

Bug ID: 18216

Description: OS Provisioning on Windows NT with Service Pack versions less than 6a times out with the error message:

```
unable to locate iphlpapi.dll & index out of range.
```

Platform: Windows NT SP4

Subsystem: OS Provisioning

Error Message:

```
Name: Buildscript Failure
Description: Failure condition occurred while executing a
buildscript.
Error Details
Error ID: 38830318
Time: 04-20-04 06:34:19 PM
Hostname: gold5.goldsox.qa.opsware.com
Error Message: Windows install timed out
```

Resolution: A previous release of the Opsware System required installation of SP6a on NT4 servers because the Opsware agent installer used APIs that were only available in SP6a. The fixed agent installer no longer uses the API that was only available in SP6a. Thus, SP6a is no longer required to install the Opsware agent.

Reconcile

Bug ID: 18122

Description: On an HP-UX 10.20 server, reconciling packages that include a pre-install or post-install script fails with an error message.

Platform: HP-UX 10.20

Subsystem: Reconcile

Error Message:

```
$opsware_error: ['OpswareError', {'method': 'preReturn',
'faultString': 'wayscripts.reconcile_genericError',
'line': 2869, 'args': [], 'tb_chain': [], 'faultCode':
101, 'cascade': None, 'error_name':
'wayscripts.reconcile_genericError', 'module':
'opsware::reconcile~20::0::16.py', 'request': 'UNKNOWN',
'hostname': None, 'timeticks': 1081916662L, 'timestamp':
'14/Apr/2004 042422', 'params': {'error_messages':
['There was an error with package opsw1.test-A.01.00',
'There was an error with package opsw2.test-A.01.00']}}]
```

Resolution: Previously, a program exception would be raised if a package was not installed, but had a post-installation scripted defined. Now it works without generating a program exception.

Known Problems, Restrictions, and Workarounds in Opsware System 4.5

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

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: 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.

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

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: 19610

Description: Changing the value of the Search Domain field (found on the Network tab in Managed Servers) results in a message indicating that the job completed successfully, but the changes are not reflected in the Opsware Command Center. This can happen if the interface is configured for DHCP.

Platform: Linux AS 3.0-J

Subsystem: Network Configuration Backend

Workaround: This functions as designed. This occurs because the server is configured to use DHCP. The search domain settings received by the managed server during DHCP lease negotiation will overwrite the settings that you provide.

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: 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.

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 you 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: 18188

Description: The OS Build Agent gets deleted from the Software Repository, consequently, the server cannot be provisioned.

This is a very infrequent bug and has not been reproduced. It was observed when installation on a server was interrupted by a lab upgrade between the time the server was placed in the server pool and the attempt was made to provision it.

Platform: Windows 2000

Subsystem: OS Provisioning

Workaround: None

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: 19277

Description: Clicking on a Linux 7.2 RPM with Japanese characters in the name results in an error:

Platform: Linux 7.2

Subsystem: Software Repository

Workaround: If you want to use RPMS with international characters in the file name do the following tasks on the server where the Software Repository resides:

1. Mount disk 1 of the Opsware Installation CDs.

2. Issue these commands:

```
/lc/bin/rpm -Uvh --nodeps <path to cd>/packages/solaris/rpm-
3.0.6-LC~1.sparc64.rpm
/lc/bin/lcdepot
```

This will update the version of RPM that is installed on the server.

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 (Darma Muthiayen)

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.