Opsware® SAS 5.3

Release Notes

Corporate Headquarters

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

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

Table of Contents

Introduction to Opsware SAS 5.3

Opsware SAS 5.3 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.

Opsware SAS 5.3 includes the following new features:

- OCC Client Scheduler
- Application Configuration Management Enhancements
- OCC Client – Server Explorer Enhancements
- Server Compliance Enhancements
- Shell Audit
- New Permissions in Opsware Global Shell
- Virtualization Support
- New Operations in Opsware SAS Web Services API 2.2
- New Features in Opsware Data Center Intelligence (DCI) 1.7
- Changes In DCML Exchange Utility (DET) 2.1
- Support for New Platforms in Opsware SAS 5.2
- Internationalization
- Automated Upgrade to Opsware SAS 5.3

What's New In Opsware SAS 5.3

OCC Client Scheduler

In this release, the new OCC Client Scheduler allows you to schedule the following OCC Client jobs:

- Server Compliance Audit
- Server Compliance Snapshot
- Application Configuration Audit
- Application Configuration Push

You can schedule these jobs to run once, daily, weekly, monthly, or on a custom schedule using crontab strings. You can also choose to send an email notification on the success or failure of a job.

Application Configuration Management Enhancements

In this release, Application Configuration Management provides the following new features:

- Internationalization - Double Byte Character Support for Templates and Configuration Files: Application Configuration now supports templates and configuration files encoded in double byte characters.
- Preserve Values: This new feature allows you to preserve the values contained in the configuration file on the managed server. With this option activated, you can ensure that the managed configuration file's values will serve as default values for the template, and will be used unless overridden by values at some level of the inheritance hierarchy.
- Show Inherited Values: This feature allows you to show what values are being inherited from higher levels of inheritance hierarchy. When turned off, you will only see the values set at the current level of the application configuration

inheritance scope. When turned on, you will see both values set at the current level and those that are inherited.

- Sequence Aggregation:
- Because application configuration values can be set across many different levels in the application configuration inheritance hierarchy (also referred to as the inheritance scope), ACM now allows you to control the way sequence values are merged across inheritance scopes. For example, add some values to a sequence in the Customer scope, Group scope, and the Server scope, and all the values will be merged together to form the final sequence.
- New Sequence Aggregation Modes
- Sequence Replace: Allows you to specify that sequence values from more specific scopes completely replace those from less specific scopes. This occurs for both sequences of sets and lists.
- Sequence Append: Allows you to specify that values at more general scopes are appended (placed after) to those at more specific scopes.
- Sequence Prepend: Works the same as append, but values at more general scopes are preprended (placed before) to those at more specific scopes.
- Scheduler: You can now schedule Application Configuration Pushes and audits to run once or at regular intervals. You can also choose to send an email notification when the job has finished, or if the job ran successfully without errors.
- Data-manipulation script: This new script allows you to operate on certain configuration files which contain unreadable or otherwise unmanageable data before you perform an import, preview, or push the application configuration.

OCC Client – Server Explorer Enhancements

- Server Explorer: The OCC Client's Server Explorer now allows you to browse COM+ objects and Windows IIS Metabase for Windows managed servers.
- My Jobs: In the OCC Client My Jobs windows, users can now see their jobs or ALL jobs, depending upon new jobs permissions. Users can now edit jobs that

are scheduled ("recurring") if they created the job or they have the "Edit Job" permission.

Server Compliance Enhancements

In this release, Opsware Server Compliance provides new features, enhancements, and several bug fixes. The new features and enhancements include:

- Scheduling when you want a snapshot created (either once or as a recurring job) and specifying who you want to receive email notification about the status of the job. You can also view, edit, and delete existing snapshot schedules.
- Scheduling when you want an audit performed (either once or as a recurring job) and specifying who you want to receive email notification about the status of the job. You can also view, edit, and delete existing audit schedules.
- Browsing and selecting individual Windows Metabase settings for snapshots and audits.
- Browsing and selecting individual Windows COM+ objects for snapshots and audit.

Shell Audit

In this release, when you use the Opsware Global Shell feature to access or modify a managed server, Opsware SAS records the events performed on the server in an audit trail. The audit trail contains information about the operations that occur in the Opsware Global File System (OGFS). You can access the log files in the audit trail from the following location:

`/var/opt/OPSWmnt/audit/event/AuditArchive/`*`hostname`*`/audit.log.`*`n`*

New Permissions in Opsware Global Shell Permissions

The aaa utility has a new option (-s) to indicate that the login account on the servers (specified by -f, -c, or -g) is the same as the Opsware user name.

The following new operations can now be granted or revoked with the aaa utility:

- readServerComplus: Reads COM Plus objects as a specific login. In the OCC Client, use the Server Explorer to browse these objects on a Windows server.
- readServerMetabase: Reads IIS Metabase objects as a specific login. In the OCC Client, use the Server Explorer to browse these objects on a Windows server.

Virtualization Support

In Opsware SAS 5.3, you can install a Windows or Linux Opsware Agent on a server running VMware ESX Server 2.5. To run a Linux or Windows Opsware Agent on a server running VMware, VMware ESX Server 2.5 must support that guest OS.

For the list of Linux and Windows operating systems that the Opsware Agent runs on, see the *Opsware SAS 5.3 User's Guide*.

For the list of supported guest operating systems that you can run on VMware ESX Server 2.5, see the VMware ESX Server 2.5 documentation and data sheets.

When you install an Opsware Agent on a VMware-enabled server, the server appears in the Opsware Command Center and OCC Client as a managed Windows or Linux server. For example, if you install a Windows Opsware Agent for Windows Server 2003 and a Linux Opsware Agent for Red Hat Linux 8.0 on a WMware-enabled server, Opsware SAS will display an entry in the server lists for each of these Opsware Agent installations.

On a VMware-enabled server, the Opsware Agent is capable of performing all server management tasks. The hardware information that the Opsware Agent reports to Opsware SAS depends on how the VMware ESX Server is configured on that hardware.

New Operations in Web Services API 2.2

This release of the Web Services API has the following new features:

- New Web Services:
    - Custom Field: Manages custom field definitions and values.

    - Opsware: Retrieves information about the Web Service, such as the version and locale.
    - Server Group: Manages server groups, which are collections of servers based on rules (selection criteria) or static lists.
- New operations in the Distributed Script Web Service:
    - create: Creates a new Script object, which represents a distributed script that can be executed on managed servers.
    - delete: Deletes a Script object.
    - get: Retrieves a Script object.
    - getCurrentVersion: Retrieves the current version of a script as a ScriptVersion object.
    - getScriptText: Retrieves the text (source code) of a script's current version.
    - update: Updates the name and usage notes of a Script object.
    - updateScriptText: Updates the text (source code) of a Script object, creating a new version.
- New operation of the Node Web Service, getChangeLogList: Retrieves a list of objects that describe the changes (history) made to a node over a specified period of time
- The Opsware permissions required for the Web Service operations are now documented in the Opsware SAS Web Services API 2.2 Guide.

New Features in Data Center Intelligence (DCI) 1.7

In this release, the Public Views appendix has been updated with a new overview and relationship diagram.

Changes in DCML Exchange Utility (DET) 2.1

Since the Opsware SAS 5.1 release, the DET -c option the can no longer be used on its own and must instead be used with the export command. For example, previously, you would have cleaned out the content directory using the following command:

```
$ cbt -c <content-dir>
```

Now, the -c (or --clean) flag can only be used with the export command. For example:

```
$ cbt -e <content-dir> -c (or --clean)
```

Support for New Platforms in Opsware SAS 5.3

Opsware SAS 5.3 now supports the following operating systems for Opsware Agents:

- HP-UX 11i v2 (PA-RISC)
- HP-UX 11i v2 (Itanium)

Internationalization

Opsware SAS 5.3 allows Japanese and Korean input and then displays that content in those languages. See the sections that follow for more information.

This release has not been localized. The UI elements of the Opsware Command Center and OCC Client have not been translated into non-English languages.

Supported Japanese Operating Systems for Core Servers

You can install an Opsware SAS core on servers running the following localized (Japanese) operating systems:

- Red Hat Enterprise Linux 3.0 AS
- Solaris 9

Supported Japanese and Korean Operating Systems for Managed Servers

Opsware SAS can manage servers that run the following localized operating systems:

Japanese:

- Windows 2000, 2003
- Fujitsu Solaris 8, 9
- Solaris.8, 9, 10
- Red Hat Linux 7.3

- Red Hat Enterprise Linux 2.1 AS
- Red Hat Enterprise Linux 3.1 AS
- HP-UX 10.20, 11.00, 11.11

Korean:

- Solaris 8, 9
- Windows 2000 and 2003
- HPUX 10.20, 11.11

Supported Japanese and Korean Browsers for the Opsware Command Center

The following browser is supported:

Internet Explorer 6 running on Windows XP Pro SP2, Japanese and Korean

Supported Japanese and Korean JRE for the OCC Client

The desktop that runs the OCC Client requires the Java 2 Runtime Environment (JRE) version 1.4.2 with Java Web Start enabled. Users in non-English locales need to install the internationalized version of the JRE.

Database Requirements for Japanese and Korean Core Systems

If you install the Model Repository on a server that runs a localized Japanese or Korean operating system, the Oracle database must meet the following requirements:

- The database must be created as UTF8.
- NLS_LENGTH_SEMANTICS=CHAR must be set when database is created.
- NLS_LANG must be set correctly to LANGUAGE_TERRITORY.CHARACTERSET, where the characterset is UTF8.
- NLS_SORT=GENERIC_M must be set at the database level.

For more information on required database settings and the list of supported Oracle versions, see the Opsware SAS Deployment and Installation Guide, Appendix A.

Available Character Encodings

The Opsware Command Center and OCC Client allow you to select the encoding of file contents, package metadata, and scripts. In the encoding drop-down lists, you can select from the following items:

- Arabic (ISO-8859-6)
- Baltic (Cp1257)
- Baltic (ISO-8859-13)
- Baltic (ISO-8859-4)
- Central European (Cp1250)
- Central European (ISO-8859-2)
- Chinese Hong Kong, Taiwan (Cp950)
- Chinese Simplified (EUC-CN)
- Chinese Simplified (GB18030)
- Chinese Simplified (GBK)
- Chinese Traditional (Big5)
- Chinese Traditional (Big5-HKSCS)
- Chinese Traditional (EUC-TW)
- Cyrillic (Cp1251)
- Cyrillic (ISO-8859-5)
- Cyrillic (KOI8-R)
- English (US-ASCII)
- Greek (Cp1253)
- Greek (ISO-8859-7)
- Hebrew (Cp1255)
- Hebrew Visual (ISO-8859-8)
- Japanese (EUC-JP)
- Japanese (ISO-2022-JP)

- Japanese (Shift_JIS)
- Korean (Cp949)
- Korean (EUC-KR)
- Korean (JOHAB)
- South European (ISO-8859-3)
- Thai (TIS-620)
- Turkish (Cp1254)
- Turkish (ISO-8859-9)
- Unicode (UTF-8)
- Vietnamese (Cp1258)
- Western (Cp1252)
- Western (ISO-8859-1)
- Western (ISO-8859-15)

Specifying the Encoding in the Opsware Command Center

The following table lists the places in the Opsware Command Center where you can view or specify the character encoding.

Item Encoded	**Opsware Command Center Page Containing the Item**	**Section in User's Guide With Related Information**
scripts (upload)	New Script page, Run Distributed Script Wizard	"Character Encoding for Package Metadata and Scripts", "Creating a Script"
scripts (download)	New Script page, Run Distributed Script Wizard	"Editing, Deleting, and Downloading a Script"
package metadata	Packages page, Software	"Character Encoding for

(upload)	Install Wizard	Package Metadata and Scripts", "Creating a Script"

Specifying the Encoding in the OCC Client

The following table lists the places in the OCC Client where you can view or specify the character encoding.

Item Encoded	**OCC Client Window Containing the Item**	**Section in User's Guide With Related Information**
managed server default encoding	Properties window of Server Explorer	"Server Properties"
file contents on a managed server	Server Explorer	"Working with a Server's File System"
Windows COM+ Objects	Windows COM+ Objects window	"Windows COM+ Objects"
template file for application configuration	Configuration File Upload window	"Loading a Template File", "Editing Default Values for an Application Configuration"
file system audit results	My Jobs and Audit Result windows	"Viewing Audit Results"
source configuration file	Value Set Editor window	"Value Set Editor", "Editing Default Values for an Application Configuration" "Setting

		Application Configuration Values on a Server or Group”
package install scripts	Create Package window	"Specifying Options for New Package Content"
package metadata (Unix only)	Create Package window	"Adding New Package Content"
Global Shell and Remote Terminal sessions	Terminal and Shell Preferences window	"Terminal and Shell Preferences"
Global Shell sessions	swenc -e command	"Switching Character Encoding (swenc)", "Character Encoding for OGFS”

Locale Requirements

The core servers with the Model Repository and the Software Repository must have the en_US.UTF-8 locale installed. To display data from managed servers in various locales, the core server with the Opsware Global File System (OGFS) must have those locales installed. For more information on pre-installation requirements, see the Opsware SAS Deployment and Installation Guide.

Before launching the OCC Client, the user's locale must be set on the desktop that runs the OCC Client. For example, to view the contents of a file that contains Japanese characters, the user's locale must be set to Japanese. Also, the internationalized version of the Java Runtime Environment (JRE) must be installed on the desktop.

User Profile

The user profile (My Profile page) contains several fields related to internationalization, listed under User Preferences:

- Locale (English, Japanese, or Korean)
- Time Zone
- Long Date Format
- Short Date Format

To view Japanese or Korean characters in the OCC Client, set the Locale field in the user profile to the corresponding language. For instructions on using the profile page, see "My Profile" in the Opsware SAS User's Guide.

The Opsware Command Center supports international date and time formats. Before you can select a Japanese or Korean date format from the user profile, you must enter and save the corresponding language in the Locale field.

UTF-8 in Opsware SAS

Opsware SAS uses UTF-8 encoding for the following items:

- All Model Repository data (Oracle database)
- File names in the Software Repository
- All Opsware Command Center pages
- Communication between the Command Engine, Data Access Engine, and Web Services Data Access Engine occurs with UTF-8 encoding.
- Server search results are exported to CSV in UTF-8 format. (On Unix, you can use the iconv command convert the character encoding of the exported server search results.)

Entering Non-ASCII Characters in the Opsware Command Center

In this release, non-ASCII characters are supported in the Opsware Command Center in the following ways:

- Users can enter non-ASCII characters in all form fields throughout the Opsware Command Center.

  For example, Opsware administrators can create new Opsware users (in the Users & Groups: New User page) by entering non-ASCII characters in the name and contact information fields. Opsware users can enter non-ASCII characters in the name and notes fields in server profiles.

  In form fields, users can enter ASCII, single-byte characters (such as English alphabets, numbers, and special characters) and multi-byte characters (such as Hiragana, Katakana, and Kanji).

- The Opsware Command Center can display content in ASCII and non-ASCII (Japanese) characters throughout the interface where applicable.

  In addition to correctly displaying non-ASCII data entered by users, the Opsware Command Center can display:

    - Messages in non-ASCII characters that were returned by servers' operating systems.
    - Names of the files backed up with the Configuration Tracking Subsystem in Japanese as a result of a directory target policy entry.

Entering Non-ASCII Characters in the OCC Client

Users can enter non-ASCII characters in all form fields throughout the OCC Client using a standard Global Input Method Editor (IME). For example, when creating an audit template, the audit template can contain multi-byte characters.

In form fields, users can enter ASCII, single-byte characters (such as English alphabets, numbers, and special characters) and multi-byte characters. • The OCC Client can display content in ASCII and non-ASCII (Japanese or Korean) characters throughout the interface where applicable.

Restrictions for Non-ASCII Entry in the Opsware Command Center

In this release, non-ASCII characters are supported in the Opsware Command Center, with the following exceptions:

- The forms in the following areas of the Opsware Command Center accept only ASCII-character data entry:
    - Environment ► Service Levels | Opsware
    - Administration ► System Configuration *(only accessible by Opsware administrators)*
    - Administration ► Opsware *(only accessible by Opsware administrators)*
- The Short Name fields when creating a new customer and new facility are limited to ASCII characters due to character restrictions for the fields.
- When entering non-ASCII characters in Opsware Command Center form fields, you could receive an error message when you enter long text strings (for example, 17 or more non-ASCII characters). The Opsware Command Center verifies the character length of the text strings, while the Opsware Model Repository database stores the data in bytes. For non-ASCII characters, these lengths will not match each other. If you receive an error message, shorten the length of the text string you entered in the field.

Internationalization Limitations

The OCC Client does not support multiple languages for multi-byte characters. (This limitation does not apply to the file contents displayed by the Server Explorer.) For example, if a user is logged in under the English locale, the OCC Client cannot display Japanese, Korean, or Chinese characters. If a user is logged in under the Japanese locale, the OCC Client can display Japanese and English characters, but not Korean or Chinese.

The OCC Client relies on the Java Runtime Environment (JRE) 1.4.2, which has the following limitation: Starting a Java application in one locale may not allow the correct

characters to be shown from a code set in another locale. These characters may not be shown even if the correct fonts for the new locale are installed on the client.

The properties page of the Server Explorer includes an Encoding field. To report this encoding, the Agent must be from Opsware SAS 5.2 or 5.3. Agents from earlier versions of Opsware SAS do not report the encoding of a managed server.

The Opsware user name and password cannot contain multi-byte characters.

Bi-directional characters are not supported.

The IDK (ismtool) only runs on English servers.

The Visual Packaging server only runs on English versions of Windows.

The following features of the Opsware Command Center do not support international date and time formats:

- Configuration Tracking Subsystem
- Code Deployment Subsystem

  (In the previous releases, these subsystems did *not* display date/time values using the format specified in users' profiles.)

- In the Opsware wizards, the fields to enter a date and time to schedule an operation do *not* display the dates and times in international date and time format. However, once an operation is scheduled, the "Start Time" column in a user's My Jobs list shows the date and time format in the international date and time format.

For other limitations, see the "Known Problems" section of this document.

Automated Upgrade to Opsware SAS 5.3

In Opsware SAS 5.3, you can upgrade your Opsware installation to this release.

Opsware SAS 5.3 supports the following upgrade paths:

• Upgrading a Standalone Core from 4.8 to 5.3

• Upgrading a Multimaster Mesh from 4.8 to 5.3

• Upgrading Opsware Satellites from 4.8 to 5.3

- Upgrading a Standalone Core from 5.1 to 5.3
- Upgrading a Multimaster Mesh from 5.1 to 5.3
- Upgrading an Opsware Satellite from 5.1 to 5.3
- Upgrading a Standalone Core from 5.2 to 5.3
- Upgrading a Multimaster Mesh from 5.2 to 5.3
- Upgrading an Opsware Satellite from 5.2 to 5.3

Contact your Opsware Support Representative for information about upgrading to Opsware SAS 5.3.

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 SAS 5.3 supports. For complete information on package types and file types, see Chapter "Package Management" in the *Opsware SAS 5.3 Configuration Guide*.

Operating System and Version	Package Type	File Types
SPARC-processor-based hardware (sun4u, sun4us)		
Solaris 6, 7, 8, 9, and 10	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), Red Hat Enterprise Linux 2.1 AS/ES/WS, Red Hat Enterprise Linux 3 AS/ES/WS, Red Hat Enterprise Linux 4 AS/ES/WS,	RPM	.rpm
SUSE Linux (Enterprise Server 8.0, Standard Server 8.0, Enterprise Server 9.0)	RPM	.rpm
Microsoft Windows (NT 4.0, Windows 2000 Server Family, Windows Server 2003)	Hotfix	.exe

Operating System and Version	Package Type	File Types
	Service Pack	.exe
	MSI	.msi
	ZIP	.zip
	Security Patch	.exe
	Windows Utility	.exe
	Microsoft Patch Database	.xml, .cab
IBM-POWER-processor-based hardware		
IBM AIX (4.3, 5.1, 5.2, 5.3)	RPM	.rpm
	LPP	.bff
	Base Fileset	N/A
	Update Fileset	N/A
	APAR	N/A
	Maintenance Level	N/A
HP PA-RISC-processor-based hardware		
HP-UX (10.20, 11.00, 11.11/11i v1/11i v2)	Depot	.tar
	Product	N/A
	Fileset	N/A
	Patch Product	N/A
	Patch File	N/A
HP PA-Itanium-processor-based hardware		
HP-UX 11i v2	Depot	.tar

***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.*

Note: For the supported operating systems for Opsware Agents, Opsware SAS supports Red Hat Linux 3 AS/WS/ES and Red Hat Linux 4 AS/WS/ES on both 32 bit and 64 bit x 86 architecture. All other versions of Red Hat Linux are supported on 32 bit architecture only.

Supported Browsers

The Opsware SAS 5.3 supports the following browsers:

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

Supported Core Operating Systems

The following table lists the supported operating systems for the Opsware core components (other than the Global File System Server). The Global File System

server can be installed only on Red Hat Enterprise Linux 3 AS. Therefore, a single-server installation is supported only on Red Hat Enterprise Linux 3 AS.

Supported Operating System for Opsware core	Versions
Sun Solaris	Solaris 8 (on SPARC) Solaris 9 (on SPARC)
Red Hat Linux	Red Hat Enterprise Linux 3AS (32 bit)

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

Supported Operating System for Opsware Satellite	Versions
Sun Solaris	Solaris 9 (on SPARC)
Red Hat Linux	Red Hat Enterprise Linux 3AS (32 bit)

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

Supported Installations

The Opsware SAS 5.3 release supports the following installations:

- First time, from-scratch installation of a stand-alone core
- First time, from-scratch installation of a multimaster core
- First time, from-scratch installation of a Satellite
- Upgrade from Opsware SAS 4.8 to Opsware SAS 5.3 or Opsware SAS 5.1 to Opsware SAS 5.3 or Opsware SAS 5.2 to Opsware SAS 5.3. Refer to the *Opsware SAS 5.3 Upgrade Guide* for more information.

Documentation

This release comes with the following documentation:

- *Opsware SAS 5.3 Release Notes*
- *Planning Deployments for Opsware SAS 5.3*
- *Opsware SAS 5.3 Deployment and Installation Guide*
- *Opsware SAS 5.3 Configuration Guide*
- *Opsware SAS 5.3 Administration Guide*
- *Opsware SAS 5.3 User's Guide*
- *Opsware Data Center Intelligence 1.7 Administrator's Guide*
- *Opsware SAS DCML Exchange Tool 2.1 Reference Guide*
- *OCLI 2.0 Reference Guide*
- *Opsware SAS Web Services API 2.2 Guide*
- *Opsware SAS Intelligent Software Module (ISM) Development Kit 2.0 Guide*
- *CML Tutorial for Opsware SAS 5.3*

The Opsware SAS documentation is available online at
https://download.opsware.com/kb/category.jspa?categoryID=20

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

Opsware Agent Compatibility

The majority of the Opsware Command Center features for Opsware SAS 5.3 are compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 5.3 features with Opsware Agent versions prior to 5.3 yielded the following results for the features in the Opsware Command Center Client.

OCC Client Features

The following features in the OCC Client are compatible with Opsware Agents 5.1 and later:

- Application Configuration
- Visual Packager
- Server Browser
- Server Compliance
- Global Shell
- Opsware Discovery and Agent Deployment
- OCC Client Scheduler

To access the Services functionality in the Server Browser feature, you must upgrade to Opsware Agent 5.2 or later.

What's Fixed in Opsware SAS 5.3

The following bugs have a severity level of Critical or Major and are fixed in Opsware SAS 5.3.

Command Engine

Bug ID: 29900

Description: If the Command Engine cannot contact the Web Services Data Access Engine, it does not log the error.

Platform: Independent

Subsystem: Core - Command Engine

Resolution: Fixed. The Command Engine logs a waybot.NoReachableTwists error in the `/var/lc/waybot/waybot.err` file.

This error indicates the IPs that were tried and the list of known bad IPs.

Opsware Agent

Bug ID: 26687

Description: The AIX Opsware Agent did not detect when it successfully exited and it did not detect fatal errors in its process.

Subsystem: Opsware Agent

Platform: AIX

Resolution: Fixed.

Bug ID: 29435

Description: In order to deploy an Opsware Agent, the Opsware Discovery and Deployment feature, will try to log in to each of the selected unmanaged server with the specified user name and password. If the password specified contained “$”, ODAD would fail to log in to the unmanaged server.

Subsystem: OCC Client - ODAD

Platform: Platform Independent

Resolution: Fixed.

Bug ID: 29895

Description: If there were more than one agent-side gateways in a core, Opsware Discovery and Agent Deployment feature failed to deploy agents to a Windows server.

Subsystem: OCC Client - ODAD

Platform: Windows

Resolution: This has been fixed in Opsware SAS 5.3.

Opsware Command Center

Bug ID: 29162

Description: When a new Facility or Customer was created in an upgraded Opsware SAS 5.2 core (upgraded from Opsware SAS 4.8), the Facility or Customer did not show up in the OCC. This behavior was only observed when the Web Services Date Access Engine was not responding or running when you launch the OCC.

Subsystem: Opsware Command Center

Platform: Independent

Resolution: Fixed.

Bug ID: 29273

Description: Moving a node in the Software Tree to a destination node which has more than 100 subnodes, resulted in an error.

Subsystem: Opsware Command Center

Platform: Platform Independent

Resolution: Fixed. You can use the move Node wizard to move a node a destination node which has more than 100 subnodes.

Opsware Command Center Client

Bug ID: 29039

Description: If you were trying to create a snapshot and a file's owner or user group did not have text representation on a Unix operating system, the following error displayed:

```
NameError: display_warning
```

This meant that files with unknown users and user groups would not have their information set. Because this was only a warning, the snapshot process still succeeded.

Platform: Platform Independent

Subsystem: OCC Client - Audit & Compliance

Resolution: Fixed. Unknown users and user groups are recorded as their numeric uid and gid, respectively.

Bug ID: 29046

Description: The creating a package process sometimes failed when a Red Hat Enterprise Linux AS 4 server was used as a packaging server, regardless of whether a second packaging server was used.

Platform: Platform Independent

Subsystem: OCC Client - Visual Packager

Resolution: Fixed in version 2.0.8 of the ISM tool.

Bug ID: 29051

Description: When you used Visual Packager to try to replace (overwrite) a file that already existed in the Software Repository you got a Database Unique Constraint Error.

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Resolution: Fixed in version 2.0.8 of the ISM tool.

Bug ID: 29053

Description: Items did not display in the Contents tab of the Create Package window when there was only one object in a category (such as File System or Installed Patches) that was first selected and then deselected in the Details tab.

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Resolution: Fixed.

Patch Management

Bug ID: 29906

Description: In the Patch Preferences tab, the Select button under Patch Options did not function correctly when you had too many products selected in the Patch Options window.

Subsystem: Patches

Platform: Platform Independent

Resolution: Fixed. You can now use the Select button to select all or a large number of entries in the Patch Options window.

Known Problems, Restrictions, and Workarounds in Opsware SAS 5.3

This section describes the workarounds to known problems in Opsware SAS 5.3.

Access and Authentication

Bug ID: 23457

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

Platform: Platform Independent

Subsystem: Access and Authentication

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

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

Bug ID: 27445

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

Platform: Platform Independent

Subsystem: Access and Authentication

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

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

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

Permission	Description
Model: Applications	Manage Application Nodes

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

Permission	Description
Model: Service Levels	Manage Service Level Nodes

To obtain the required permissions, contact your Opsware administrator.

Bug ID: 27675
Description: For delegated authentication, client certificates are not supported.
Platform: Platform Independent
Subsystem: Access and Authentication
Symptom: If the external LDAP server is configured to require client certificates, then the Opsware SAS is unable to successfully communicate with the external LDAP server. Specifying client certification properties in the twist.conf file does not help, because the external LDAP server expects a distinct client certificate per user.
Workaround: When connecting to an external LDAP server, use either of the following approaches:

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

Code Deployment

Bug ID: 27529
Description: Run sequence fails if the user is not assigned to the CDS History Viewer group.
Platform: Platform Independent

Subsystem: Code Deployment

Symptom: When a user belonging to the CDS Production Sequence Performer group attempts to run a sequence, the sequence fails leading to the following error:
The input you entered was invalid or you tried to access a resource not available to you. Please check the URL entered or click the back button and check your input.

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

Configuration Tracking

Bug ID: 22674

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

Platform: Platform Independent

Subsystem: Configuration Tracking

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

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

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

Content

Bug ID: 28117

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

Platform: Unix/Linux

Subsystem: Content – Application Configuration

Symptom: At this time, application configurations will not start services that are not already running. In the event you wish to configure a Unix or Linux service that is not already running on a system, please start the service before using application

configurations or you may get an error from the application configuration post-script execution. This error can be ignored, as the configuration has in fact been pushed to the server, but the service has not been started.

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

DCML Exchange Tool

Bug ID: 25383

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

Platform: Platform Independent

Subsystem: DET

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

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

Bug ID: 27940

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

Platform: Platform Independent

Subsystem: DET

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

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

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

Bug ID: 28775

Description: Export Package Filter Windows Hotfix and Service Pack Issue

Platform: Windows Packages

Subsystem: DCML Exchange Utility (DET)

Symptom: For Microsoft Hotfixes and service packs, it is possible that the Microsoft package you want to export has not yet had its binary file uploaded, even though the package shows as existing in the core. For example, a user may have uploaded the Microsoft Patch Database to the core, but not yet uploaded the actual binary file of the package. In this case, a unit record for the package will have been created in the Opsware model, but there is no content to export. In this case, if you try to export the package content using the Package Export Filter, the content of the Microsoft package will not be exported.

Workaround: Make sure that before you export a Microsoft Hotfix package or Service Pack package the package has previously been uploaded to the core you are exporting the content from.

Bug ID: 30021

Description: Non-ASCII characters in the target directory name for Configuration Tracking are not displayed properly after a DET import.

Platform: Platform Independent

Subsystem: DET

Symptom: If you try to use the DET import to import an application node with configuration tracking policy set and if the target file or the directory name has non-ASCII characters, then after the import, the file or directory name containing the non-ASCII characters is not displayed correctly.

Workaround: None.

Bug ID: 30600

Description: Import error occurrs during custom fields import when target core has same custom field name.

Platform: Any

Subsystem: DET Import

Summary: When importing a custom field, the error "OpswareError:spin.DBUniqueConstraintError" may be returned if the target core already has a custom field with the same display name.

Workaround: Ensure there is are no conflicting display names, or rename the display name prior to importing.

Installer

Bug ID: 27268

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

Platform: Linux

Subsystem: Installer

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

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

Bug ID: 28663

Description: Installation of an Opsware Satellite fails if you try to reinstall the Satellite after uninstalling it.

Platform: Platform Independent

Subsystem: Installer

Symptom: After uninstalling an Opsware Satellite, if you try to reinstall the Satellite again without deactivating the Opsware Agent from the core, the installation fails with the following error:

```
OpswareError:
args:  ()
error_name:  spin.permissions
faultCode:  9
faultString:  spin.permissions
hostname:  thunder1.thunder.qa.opsware.com
line:  6861
method:  updateDevice
module:  spinmethods.py
params:  {'msg': 'Attempt to register server with bootstrap
cert after crypto has been generated and with allow_recert
set to 0.'}
```

Workaround: After you uninstall an Opsware Satellite, log in to the Opsware Command Center and deactivate the server before reinstalling the Satellite again.

Bug ID: 28730

Description: Error when installing the OCC component on Solaris

Platform: Solaris

Subsystem: Installer

Symptom: This problem occurs when the Opsware Installer is installing the Opsware Command Center component on a core server. Although it successfully installs the occapp package, the Opsware Installer displays these lines and exits:

```
package occapp is not installed
<time-stamp> Component installation script encountered an
error
```

Workaround: Check to see if the executable rpm (or a symbolic link) exists in one of the following directories:

```
/bin
/usr/bin
```

```
/sbin
/usr/sbin
/usr/local/bin
```

If does exist in one of these directories, remove or rename the file and run the Opsware Installer again.

Bug ID: 28824

Description: Cannot connect to a Windows 2003 server using the Remote Terminal option of the OCC Client.

Subsystem: Installer

Platform: Independent

Symptom: From the OCC Client select the server and from the Actions menu select Remote Terminal. The following error message is displayed:

```
The connection was ended because of a network error.
```

Workaround: This error occurs if the EgressFilter entry in the core Opsware Gateway properties file is incorrect. (The entry in the Gateway properties file provided by the Opsware Installer is correct, so this error occurs only if you've edited the file manually.) To fix this error, log into the core server running the Opsware Gateway and edit this file:

```
/var/opt/OPSWgw/cgw0-<facility>/opswgw.properties
```

Include the following entry in the properties file:

```
opswgw.EgressFilter=tcp:*:3389:HUB:
```

Restart the Opsware Gateway:

```
/etc/init.d/opswgw-cgw-<facility> restart
```

Bug ID: 29041

Description: Uninstaller fails if it uses a response file with no oi.components.

Subsystem: Installer

Platform: Independent

Symptom: When uninstalling a core, the uninstaller might generate the following traceback message:

```
Traceback (innermost last):
  File "./manage_opsware.py", line 183, in manage_opsware
  File "./manage_opsware.py", line 344, in validateParams
  File "./manage_opsware.py", line 325, in
getComponentParams
KeyError: oi.components

[time-stamp] Opsware Installer has encountered an error:
[time-stamp] Error Type : exceptions.KeyError
[time-stamp] Error Value: oi.components
[time-stamp] Exiting Opsware Installer.
```

Workaround: Perform the following steps:

1. Add an oi.components section to the response file. For example:
   %oi.components docs
2. Run the uninstaller again.
3. After the uninstall completes, remove the oi.components section you just added. If you don't remove the oi.components section, problems may occur if you try to use the response file in the future without an action file.

Bug ID: 29161

Description: During the installation of the Opsware Global File System (OGFS), `ogfs.store.host` and `ogfs.audit.host` parameters cannot be set to any host.

Subsystem: Installer

Platform: Linux

Symptom: This problem occurs during the installation of the OGFS for the core, and the `ogfs.store.host` or `ogfs.audit.host` parameter is set to a host other than the OGFS or the Software Repository (theword).In this case, the Opsware Installer fails to install the OGFS and displays the following error message:

```
Running script hub/pre.
```

```
Mounting /var/opt/OPSWmnt/store mount:
<ip>:/cust/ogfs/store failed,
reason given by server: No such file or directory
[timestamp]
Component installation script encountered an error (exit
status 32)
[timestamp] Exiting Opsware Installer.
```

Workaround: For the `ogfs.store.host` and `ogfs.audit.host` parameters, use the default values or specify the host of either the OGFS or the Software Repository.

Intelligent Software Module (ISM) Development Kit

Bug ID: 30106

Description: The ismusertool cannot upload an ISM from a managed server that communicates with the core through an Opsware Gateway.

Subsystem: IDK

Platform: Independent

Symptom: The upload displays a traceback that includes the following lines:

```
  . .
File "/usr/local/ismtool/lib/ismtoollib/ismusertool.py",
line 293,
  in cmdline()
File "/usr/local/ismtool/lib/ismtoollib/ismusertool.py",
line 269,
  in cmdline checkIsmUpdateRole()
. . .
```

Could not set up a tunnel through any of [(<ip-address>, 3002)]

Workaround: Run ismusertool as the Opsware admin user on a server that does not communicate with the core through a Gateway.

Bug ID: 30156

Description: Setting allowservers on an uploaded ISM causes a data integrity error.

Subsystem: IDK

Platform: Independent

Symptom: The following example commands show how this problem might occur:

1. Create an ISM node with a multi-level opswpath such as

   /System Utilities/${NAME}/${VERSION}/${PLATFORM}.

2. ismtool --addPathProp allowservers --propValue 1 ismx
3. ismtool --upload ismx
4. Run a data integrity test on the core.

The test reports an error because the parent node of ismx has an allowservers value of 0. That is, the parent node does not allow servers to be assigned to it.

Workaround: Make sure that the allowservers values
of the uploaded ISM node and the parent node are the same.

Operating System Provisioning

Bug ID: 26125

Description:

Platform: Platform Independent

Subsystem: OS Provisioning

Symptom: When you reprovision a server, the Opsware Command Center (OCC) uses the display name when displaying a server, whereas the Opsware Command Center Client (OCC Client) uses the hostname when displaying a server.

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

Workaround: None

Opsware Agent

Bug ID: 26747

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

Platform: Windows

Subsystem: Agent

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

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

Bug ID: 27590

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

Platform: Windows NT

Subsystem: Agent

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

Workaround: None.

Bug ID: 28176

Description: ogshcap.dll file is not available if an Opsware Agent is uninstalled and reinstalled without restarting the server.

Platform: Windows

Subsystem: Opsware Agent

Symptom: During Opsware Agent uninstallation on a Windows server, the Agent Installer tries to remove the ogshcap.dll file from the following location:

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

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

After uninstalling the Opsware Agent, if you reinstall it without restarting the server, the ogshcap.dll file does not get copied. During the next reboot you will not be able to access the server's file system since ogshcap.dll file is no longer available.

Workaround: Restart the server after the uninstalling the Opsware Agent and before reinstalling the Opsware Agent.

Bug ID: 28950

Description: Unable to Deploy Opsware Agents to Windows server after manually uninstalling and reinstalling the Opsware Agent on the Windows Agent Deployment Helper server.

Platform: Windows

Subsystem: OCC Client - ODAD

Symptom: If you manually uninstall the Opsware Agent on a server that is the Windows Agent Deployment Helper, and then reinstall the Opsware Agent on that server, the Opsware Discovery and Agent Deployment (ODAD) feature will be unable to deploy agents to Windows servers. Deployment to UNIX-based servers will not be affected.

Workaround: After uninstalling an Opsware Agent perform the following steps:

1. On the Agent Deployment Helper server, log in and use "Add/Remove Programs" to remove the Windows Agent Deployment Helper application.
2. If you did not deactivate and delete the server from Opsware SAS, two servers registered with the same hostname. The status of the old server will be UNREACHABLE. With the OCC and deactivate, then delete the old server
3. Exit any OCC Client applications that may be running.
4. Perform the procedure for installing the Windows Agent Deployment Helper. See "Installing Windows Agent Deployment Helper" in the Opsware SAS 5.2 Deployment and Installation Guide for step by step instructions on how to install Windows Agent Deployment Helper.
   After these steps are performed, the ODAD feature should be able to deploy to Windows servers.

Bug ID: 29075

Description: ODAD fails to deploy Opsware Agents to a Windows server which previously had the Windows Agent Deployment Helper installed

Platform: Windows

Subsystem: OCC Client – ODAD

Symptom: Deploying an Opsware Agent using the Opsware Discovery and Agent Deployment (ODAD) feature to a Windows server which previously had the Windows Agent Deployment Helper installed fails with an error.

Workaround: Perform the following steps before you deploy Opsware Agents to a Windows server which previously had the Windows Agent Deployment Helper installed:

1. Log in to the Windows Server
2. Navigate to Control Panel > Network and Dial up Connections.
3. Disable the adapters created by Windows Agent Deployment Helper. These adapters will be labeled as “ADT Helper <n>, where <n> is a number”.

Bug ID: 29395

Description: Opsware Discovery and Agent Deployment feature is unable to discover a realm, if the display name of the realm is changed.

Subsystem: OCC Client - ODAD

Platform: Platform Independent

Symptom: If the display name of a realm is changed, then the Opsware Discovery and Agent Deployment feature is unable to discover the realm. As a result in the OCC Client the realm is not displayed in the Scan in drop-down list.

Workaround: None. Do not the change the display name of the realm.

Bug ID: 29735

Description: The Unmanaged Server page appears, when you open a managed server in the Agent Deployment – OCC Client page.

Subsystem: OCC Client - ODAD

Platform: Platform Independent

Symptom: After successfully deploying Opsware Agents using ODAD, the status of the server in the server list is updated to a managed server. In the Agent Deployment – OCC Client page when you open the managed server the Unmanaged Server page for that server appears.

Workaround: None.

Bug ID: 29748

Description: Opsware Discovery and Agent Deployment (ODAD) fails if sudo or su is not in the user's PATH on the unmanaged server.

Subsystem: OCC Client - ODAD

Platform: Platform Independent

Symptom: When you use sudo to log in to an unmanaged server, deploying Opsware Agents using ODAD fails, if sudo or su is not in your PATH on the unmanaged server.

Workaround: None. When you use sudo to log in to an unmanaged server, verify that the sudo or su is in your PATH on the unmanaged server.

Bug ID: 29934

Description: ODAD may not accurately AIX 5.3 during a network scan.

Subsystem: OCC Client - ODAD

Platform: Platform Independent

Symptom: While performing a network scan to identify servers in which to install an Opsware Agent, ODAD may not be able to identify AIX 5.3 accurately.

Workaround: None.

Bug ID: 30303

Description: Sometimes Opsware Discovery and Agent Deployment reports a server to be managed by Opsware, even though it not managed by Opsware.

Subsystem: OCC Client - ODAD

Platform: Platform Independent

Symptom: A server is considered to be under Opsware management if the Opsware Discovery and Agent Deployment feature discovers that it is listening for TCP connections on port 1002. In some cases, this information can be incorrect.

For example, if some other software is installed and listening on port 1002, the server will be identified as managed by Opsware, when in fact it is not.

Conversely, if a server is under Opsware management, but its Opsware Agent was shut down at the time the server was scanned, the server will not be identified as managed by Opsware.

Workaround: None.

Opsware Command Center

Bug ID: 22865

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

Platform: Platform Independent

Subsystem: OCC - Manage Servers

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

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

Bug ID: 24470

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

Platform: Platform Independent

Subsystem: OCC - Wizards

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

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

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

Bug ID: 25772

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

Platform: Platform Independent

Subsystem: OCC - Manage Servers

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

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

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

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

Or

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

Bug ID: 26120

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

Platform: Platform Independent

Subsystem: OCC - System Configuration

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

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

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

Bug ID: 26382

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

Platform: Platform Independent

Subsystem: OCC **-** Server Groups

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

Workaround: None.

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

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

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

Bug ID: 27345

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

Platform: Platform Independent

Subsystem: OCC - Service Levels

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

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

Bug ID: 27718

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

Platform: Platform Independent

Subsystem: OCC - Manage Servers

Symptom: In the Opsware Command Center when you clone a server, the source server (master server) and the target servers need to have the same platform and the same customer. A twist exception appears if the master server and the target server do not have the same customer and same platform.

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

Bug ID: 27854

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

Platform: Platform Independent

Subsystem: OCC - Communication Test

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

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

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

Bug ID: 29160

Description: When you log into the Opsware Command Center, the browser prompts you twice to accept the certificate.

Subsystem: Opsware Command Center

Platform: Independent

Symptom: When you access the OCC, you are prompted twice to accept the certificate. The first prompt is related to authentication and the second one is related to the certificate name not matching the Opsware core URL.

Workaround: To access the OCC, accept the certificate twice.

Bug ID: 29201

Description: Unable to add packages to the OS definition using the Prepare Operating System Wizard.

Subsystem: Opsware Command Center - Wizard

Platform: Linux

Symptom: While creating an OS definition for Red Hat Linux using the Prepare Operating System wizard, adding packages to the OS definition in the in the Review Packages page may fail in one of the following ways:

- An error occurs when you confirm the package to add in the Review Packages page. This error asks you to retry your login.
- Only the new packages added are saved. The existing packages are not saved.

Workaround: Close the Prepare Operating System wizard. Navigate to Software - Operating System and select the created OS definition which you just created. Select the Packages tab and then add the additional packages.

Bug ID: 29293

Description: Microsoft Excel fails to open CSV files containing non-ASCII characters.

Subsystem: OCC

Platform: Platform Independent

Symptom: In the Opsware Command Center, you can generate CSV files containing information about manage servers and export it to Microsoft Excel. If the file contains non-ASCII characters, Microsoft Excel fails to open the file with the correct encoding. Since Microsoft Excel 2002 and 2003 does not support UTF-8 encoding, Unicode characters are not displayed correctly.

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

Method 1

Perform the followings steps to display non-ASCII characters correctly in Microsoft Excel:

1. Download and Save the CSV file.
2. Open the CSV file using Microsoft Windows Notepad. Windows Notepad displays non-ASCII characters correctly.
3. From the Edit menu, select Select All.
4. From the Edit menu, Select Copy
5. Open Microsoft Excel.
6. In a blank Excel worksheet, place the cursor on cell A: 1.

7. From the Excel Edit menu, select Paste. The contents from windows Notepad, is copied to Microsoft Excel.
8. In Microsoft Excel, from the Data menu select Text to Columns.
9. Change the delimiter from Tab to Comma. Click finish.
10. Save the Microsoft Excel worksheet.

Method 2

1. While importing CSV files which contain non-ASCII characters, use OpenOffice (open source software). OpenOffice supports non-ASCII characters.
2. Copy the contents of the CSV file to a blank Microsoft Excel worksheet to display non-ASCII characters correctly.

Bug ID: 29568
Description: A user belonging to the Administrators group can create a customer but does not have write access to resources associated with the customer.
Subsystem: OCC - Customers
Platform: Independent
Symptom: A user who belongs to the Administrators group creates a customer. In the Opsware Command Center, the user's Profile indicates that all customer accounts are readable and writeable. However, the user does not have access to resources (such as packages) associated with the customer. For example, in the OCC Client, the user cannot view the newly created customer in the Customer Assignment field of the Create Package window.
Workaround: Assign the user to a group that has read and write access to the customer.

Bug ID: 29681
Description: Agent caches old locale even after the locale is changed.
Subsystem: Opsware Command Center - DSE
Platform: Independent

Symptom: Change the locale of a managed server and run a DSE that echoes multi-byte characters that require the new locale. On the Script Output tab these characters appear as question marks.

Workaround: Restart the Agent on the managed server where you've changed the locale and then run the DSE script again.

Bug ID: 29971

Description: Opsware Command Center does not state that non-ASCII passwords are invalid.

Subsystem: Opsware Command Center

Platform: Independent

Symptom: In the Profile Editor window or the Change My Password window, if you enter non-ASCII characters in the password field, the following error message appears: You have included an invalid character in the password.

Workaround: Use only ASCII characters in the password.

Bug ID: 30515

Description: A JAVAscript error occurs when you create a custom attribute for a server group with a "\" at the end of the custom attribute name.

Subsystem: OCC – Custom Attributes

Platform: Platform Independent

Symptom: If you create a custom attribute for a server group with a "\" at the end of the custom attribute name, a JAVAscript error occurs. As a result no subsequent operations like adding, deleting, or editing a custom attribute can be performed for that server group.

Workaround: When you create a custom attribute for a server group, do not use "\" at the end of the custom attribute name.

If case you create a custom attribute for a server group with "\" at the end of the custom attribute name, delete the server group and create a new one.

Bug ID: 30167

Description: The psrvr.properties file includes entries for pref.occ.support.href and pref.occ.support.text, which specify the support link at the bottom of the Opsware

Command Center. Non-ASCII characters are entered for pref.occ.support.text are not displayed correctly by the Opsware Command Center.

Subsystem: Opsware Command Center

Platform: Independent

Symptom: In the link displayed by the Opsware Command Center, the non-ASCII characters appear as boxes. Also, the link does not work.

Workaround: If you edit the psrvr.properties file with a text editor, to insert non-ASCII characters, convert the characters to UTF-8 with the Java native2ascii tool.

Opsware Command Center Client

Bug ID: 25904

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

Platform: Platform Independent

Subsystem: OCC Client **-** Global Shell

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

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

Bug ID: 26033

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

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

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

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

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

Bug ID: 26115

Description: Leaving required Value Set Editor element values will delete element line in configuration file when previewed or pushed.

Subsystem: OCC Client - Application Configuration

Platform: OS Independent

Symptom: If a required Value Set element is left blank, the application configuration will become invalid and if the application configuration is pushed, the element in the configuration file on the server might be deleted.

Workaround: Do not leave required Value Set Editor elements empty, or the required value will be removed from the configuration file when previewed or pushed. The exception to this is optional blocks, which do not have to have require values entered, unless another field in that block has a value entered.

Bug ID: 26858

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

Platform: Platform Independent

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

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

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

Bug ID: 27211

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

Platform: Platform Independent

Subsystem: OCC Client

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

Workaround: None.

Bug ID: 27214

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

Platform: Platform Independent

Subsystem: OCC Client

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

Workaround: None.

Bug ID: 27276

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

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

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

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

Bug ID: 27454

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

Platform: Platform Independent

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

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

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

Bug ID: 27586

Description: Renaming filenames limitation in Global Shell, OCC Client Server Browser/File System.

Platform: Platform Independent.

Subsystem: OCC Client - Global Shell, OCC Client Server Browser/File System

Symptom: Using the Global Shell or OCC Client Server Browser/File System to rename an existing filename on a Windows managed server will fail - even if you answer "Yes" to the prompt to overwrite dialog. This failure will occur even if your user has write permission to the file system and the destination file is writable.

Workaround: To copy "file1" to an existing file called "file2" in C:\TEMP.

1. Open the global shell.
2. Navigate to the directory containing the file you want to rename:
   cd /opsw/Servers/@/foo.server/files/Administrator/C/TEMP
3. Delete the target file:
   rm file2
4. Rename (move) the source file to the target:
   mv file1 file2

ID: 27693

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

Platform: Independent

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

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

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

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

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

Bug ID: 27733

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

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

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

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

Bug ID: 27806

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

Platform: Platform Independent

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

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

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

Bug ID: 27815

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

Platform: Platform Independent

Subsystem: OCC Client **-** Visual Packager

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

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

Bug ID: 28001

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

Platform: Platform Independent

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

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

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

to a target file that is:

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

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

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

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

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

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

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

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

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

Bug ID: 28054

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

Platform: Platform Independent

Subsystem: OCC Client - Opsware Global File System

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

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

Bug ID: 28165

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

Platform: Platform Independent

Subsystem: OCC Client

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

```
An error occurred while launching/running the application.
Title: OCC Client
Vendor: Opsware Inc.
```

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

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

Bug ID: 28774

Description: When the packaging server resides in an Opsware Satellite (behind a Software Repository Cache), the create package process fails.

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Symptom: If you try to create a package when the packaging server resides in an Opsware Satellite (behind a Software Repository Cache), the following error occurs:

```
Error Encountered
SUMMARY:
Name: Upload To Software Repository Cache Prohibited
Description: Uploads to Opsware Software Repository Caches
are prohibited
Solution: Upload the package to an Opsware Software
Repository in an Opsware Core.
```

Workaround: The Visual Packager feature does not support uploads to the Software Repository Cache (which is an Opsware Satellite component that contains local copies of files). Therefore, if the packaging server resides in a Satellite, Visual Packager will not work. Do not configure a packaging server to be behind an Opsware Satellite with a Software Repository Cache configuration. Set up the packaging server in an Opsware core so that you will be able to upload packages to the Software Repository.

Bug ID: 28969

Description: When a snapshot or audit fails to upload to the Software Repository, the error message does not tell you to check the disk space on the Software Repository.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Symptom: The snapshot or audit progress status bar displays that the process is uploading the snapshot or audit to the Software Repository and then the job fails.

Workaround: When this error occurs, check the available disk space on the Software Repository.

Bug ID: 29067

Subsystem: OCC Client - Application Configuration, Jobs Window

Platform: Independent

Description: In the Audit Application Configurations job window, the Server Details area might report that all "Configurations are in compliance". However, the Servers area of the same job might show the out-of-sync icons.

Workaround: This is a known caching issue. The cache has not caught up with the latest update on the server. After a few minutes, open the window again and the correct icons will display.

Bug ID: 29136

Description: For Application Configurations that use JScript or VBScript pre- or post-install and post-error scripts, the push operation will succeed although the scripts fail.

Subsystem: OCC Client - Application Configuration

Symptom: When pushing an application configuration that contains a JScript or VBScript pre- or post-install and post-error scripts, the push succeeds even though the scripts fail. In these cases, the push ignores the scripts altogether. The application configuration does not catch the failure of the scripts and allows the push to complete without errors.

Workaround: The author of these types of scripts must make sure the scripts are free of errors to detect possible failures, and have the script forcibly return a non-zero exit status by invoking WScript.Quit(<status>).

Bug ID: 29192/29237

Description: Error when you open a terminal window for a Windows or Unix server.

Subsystem: OCC Client – Remote Terminal, Global Shell

Platform: Independent

Symptom: In the OCC Client you can use the Remote Terminal feature to open a terminal window for a Unix or Windows server and the Global Shell feature to open a terminal window for Opsware Global File System (OGFS). If the Remote Terminal session or the Global shell session for server times out or is disconnected, the following error displays:

```
An internal error has occurred.  See the console log for
details.
```

Workaround: Restart the OCC Client and then open a new terminal window for a Windows or Unix server.

Bug ID: 29211

Description: Revert fails if the managed server contains the backup configuration file.

Subsystem: OCC Client -ACM

Platform: Independent

Symptom: If an Opsware core contains multiple versions of a configuration file, and when you revert one of the versions of the configuration file to a previous state, a backup of the configuration file is created in the Opsware-managed server. If you want to revert the other versions of the same configuration file, revert fails if the managed server contains the backup configuration file.

Workaround: Remove the backup configuration file from the managed server and re-try to revert to the previous state.

Bug ID: 29335

Description: Error is given when trying to view contents of a file, stating "unsupported charset"

Platform: Platform Independent

Subsystem: OCC Client

Symptom: When viewing a file contents that is in multibyte characters, and JRE was installed before the special fonts were installed on the server, the contents of the file are garbled and an error is given.

Workaround: This error is caused when the JRE is installed BEFORE the multibyte fonts are loaded on the local system. To solve this error, you will need to uninstall JRE, and then relaunch the OCC Client.

Instructions:

1) Close the OCC Client.

2) Open "Add/Remove Programs"

3) Remove all "Java 2 Runtime Environment, SE v1.4.2_XX" and "Java 2 SDK, SE v1.4.2_XX" programs.

4) Close the Control Panel

5) Access OCC Client again using the Opsware Command Center and go to the home page

6) Click the Launch OCC Client link.

7) You will be prompted to install JRE if you use Internet Explorer to access OCC; follow instructions to install the 1.4.2 JRE.

8) When finished, the OCC Client login dialog should appear.

To reinstall Asian language fonts, follow these instructions:

1) Open the Control Panel

2) Open "Regional and Language Options"

3) Click/select the "Languages" tab

4) Make sure the "Install files for East Asian Languages" checkbox is checked

5) Click the Apply button; dialogs will display and the fonts will install. Wait until installation is finished.

6) Click OK to close the "Regional and Language Options" dialog.

7) Relaunch the OCC Client.

Bug ID: 29374

Description: When a Windows registry key and a value have the same name and exist in the level in the registry hierarchy, only the registry key is displayed in the Global Shell terminal and in the Server Explorer registry browser.

Subsystem: OCC Client – Global Shell

Platform: Independent

Symptom: Only the Windows registry key is displayed in the Global Shell terminal and in the Server Explorer registry when the registry key and value have the same name and exist in the level in the registry hierarchy.
Workaround: None.

Bug ID: 29382
Description: Import Values into Application Configuration incorrectly logged as a "preview"
Platform: Platform Independent
Subsystem: OCC Client- OGFS
Symptom: If you import a value set from a configuration file or application configuration into an application configuration using the Import Values button, this action will incorrectly be logged in the Hub as an application configuration Preview.
Workaround: None.

Bug ID: 29501
Description: Changing the encoding with the swenc command might cause problems for background processes.
Subsystem: OCC Client – Global Shell
Platform: Linux
Symptom: In a Global Shell session, change the encoding with the swenc command. Background processes that are running in the Global Shell session might fail.
Workaround: Wait until background processes have completed before changing the encoding with swenc.

Bug ID: 29521
Description: No information is logged in the audit trail log after you close the Global Shell window by clicking the X button.
Subsystem: OCC Client – Global Shell
Platform: Independent
Symptom: There is no information in the audit trail log after you close the Global Shell window by clicking the X button in the upper right corner of the window.

Workaround: End your Global Shell session and Remote Terminal session by exiting the shell (ctrl-d or exit in bash, similar in other shells) rather than closing the window by clicking the X button. If you do not do this, the audit message that corresponds to the end of the session will still get logged, but not until after you log off the OCC Client.

Bug ID: 29872

Description: Visual Packager supports only ASCII characters in the application node path name.

Subsystem: OCC Client - Visual Packager

Platform: Platform Independent

Symptom: If you include non-ASCII characters in the application node Name in the Specify Application window, Visual Packager creates the new node in the Software Tree (with packages attached) and each non-ASCII character displays as a question mark (?).

Workaround: None.

Bug ID: 29980

Description: In CML sequence aggregation, namespace sequences append when either sequence-append or sequence-prepend is specified instead of prepending when prepend is specified.

Platform: Platform Independent

Subsystem: Application Configuration

Symptom: In some cases, even though sequence-prepend is specified for a namespace sequence, the sequence will use sequence-append. The CML contained in this tag definition would be affected by this bug:

If the CML contained this tag definition:

```
@sequenceA;unordered-namespace-set@
ITEM: @.item1@ @item2@
```

This sequence would append and prepend as specified:

```
@sequenceB;unordered-string-set;;;field-delimiter-is-eol@
ITEM: @.@
```

Workaround: Try to simplify namespace sequences into string sequences; in the above example, you would replace sequenceA with sequenceB.

Bug ID: 30029
Description: Cursor remains an hour glass after opening a scheduled job
Platform: Platform Independent
Subsystem: OCC Client - My Jobs
Symptom: In the My Jobs window, double clicking a scheduled job opens up the Schedule Job dialog window. However, the mouse pointer remains an hour glass.
Workaround: Move the mouse around a few times and the cursor reverts back to an arrow.

Bug ID: 30109
Description: Actions cannot be performed on services with names containing non-ASCII characters.
Subsystem: OCC Client - Server Explorer
Platform: Linux
Symptom: In the OCC Client, the Services window of the Server Explorer enables you to change run levels and perform actions such as start and stop. However, if the service name contains non-ASCII characters, you cannot use the Services window to change the run levels or perform the actions.
Workaround: Use only ASCII characters in service names.

Bug ID: 30265
Description: Data-manipulation script in application configuration can only be executed on individual servers.
Platform: Platform Independent
Subsystem: OCC Client **-** Application Configuration
Symptom: If you have a data-manipulation script inside an application configuration, you will only be able to run this script on individual servers, not on an entire server group from the Server Groups Browser.

Workaround: If you would like to run the data-manipulation script on a server group from inside the Server Groups Browser, you will need to run it on each individual server.

Bug ID: 30271

Description: Shift_JIS file names within a ZIP package are not displayed correctly.

Subsystem: OCC Client - Visual Packager

Platform: Windows

Symptom: With the Visual Packager of the OCC Client, upload a ZIP package that contains files whose names contain Shift_JIS characters. If you view the contents of the uploaded package in the Opsware Command Center, the Shift_JIS characters of the file names are not displayed correctly. (However, the package metadata, which is always UTF-8 on Windows, is displayed correctly.)

Workaround: Use only ASCII characters in these file names.

Bug ID: 30275

Description: An Application Configuration script fails to run if the script name has non-ASCII characters.

Subsystem: OCC Client - Application Configuration

Platform: Independent

Symptom: When you try to run the script, an error such as the following might appear:

```
Script execution failed: Code: '1', script name: ...
server id: ... stdout: ... stderr: ... cannot open
```

Workaround: Use only ASCII characters in the file names of Application Configuration scripts.

Bug ID: 30354

Description: When an Opsware user is deleted, the home directory is not deleted. If a user with the same user name is subsequently created, the new user inherits the existing home directory (and all contents).

Subsystem: OCC Client – Global Shell

Platform: Independent

Symptom: If an Opsware user is deleted and a new Opsware user is created with the same user name, the new user can view files that the previous user had in their home directory.

Workaround: Do not reuse user names. If you do reuse user names, delete the Global Shell home and tmp directories when you delete the owning user of those directories.

Bug ID: 30369

Description: Files with size 0 are not listed correctly in the OCC Client Server Explorer's file browser.

Platform: Platform Independent

Subsystem: OCC Client

Symptom: Any file with a size of zero (0) will have its properties listed incorrectly in the OCC Client's Server Explorer file browser. The file will show "Unknown" as the file type, and show an old date as the last modified date.

Workaround: None.

Bug ID: 30429

Description: If you try to create a package that includes a patch that needs to be uploaded to the Software Repository, where the Customer Assignment for the new package is not set to Customer Independent, the upload will fail.

Subsystem: OCC Client - Visual Packager

Platform: Independent

Symptom: When you try to create a package that includes a patch that needs to be uploaded to the Software Repository and the Customer Assignment for the new package is not set to Customer Independent, the patch will not be uploaded and the package will not be created.

Workaround: Change the Customer Assignment to Customer Independent to upload the patch to the Software Repository and create the new package. Patches can only be owned by Customer Independent. Only patches with the Customer Assignment of Customer Independent can be uploaded to the Software Repository.

Bug ID: 30495

Description: OCC Client not launch directly, from outside of the Opsware Command Center.

Platform: Windows 2003

Subsystem: OCC Client

Symptom: If you attempt to launch the OCC Client application on a Windows 2003 server from outside of the Opsware Command Center (for example, from your desktop), it will not launch.

Workaround: Adjusting your browser's security settings will solve this issue. Note, however, that making these changes will revert your browser's security to Windows 2000 levels.

1. From the control panel, choose Add/Remove Programs 2. Click Add/Remove Windows Components 3. Uncheck "Internet Explorer Enhanced Security Configuration"
4. Click Next as many times as necessary, and then Finish.
5. Restart your browser.

Bug ID: 30514

Description: User must belong to Administrators group to browse metabase.

Subsystem: OCC Client - Global Shell

Platform: Windows

Symptom: In a Global Shell session, a non-admin user has permission to view the `/opsw/@/<server>/metabase` subdirectory of OGFS. However, the user cannot browse metabase, and the session displays the message `"Protocol error."`

In the agent.err file, the following lines appear:

```
<timestamp> [10997] ERR  Error from Agent for unique <int>:
. . .
File ".\base\ops\shell\ogfs_wshandler.py", line 402, in run
File ".\base\ops\shell\metabase.py", line 72, in
metabase_getattr
```

Workaround: Login as a member of the Administrators group (admin).

Bug ID: 30557

Description: The Opsware user "nobody" is unable to launch the Global Shell.

Subsystem: OCC Client – Global Shell

Platform: Independent

Symptom: Create an Opsware user "nobody" and grant it self shell permissions. Log in to the OCC Client as "nobody" and try to launch the Global Shell. The telnet client briefly displays and then disappears. Try to log in as "nobody" directly on the Hub (using /opt/OPSWogfs/bin/ogsh). This also fails and no error message is displayed.

Workaround: Do not create an Opsware user called “nobody”.

Bug ID: 30559

Description: An "RFS specific error" can occur in the OGFS when you try to access the file system of a managed server, where the specified login account is disabled on the managed server. For example, the "ls /opsw/Server/@/m221.qa/files/arnold/" command fails if the login account "arnold" on server "m221.qa" is disabled.

Subsystem: OCC Client – Global Shell

Platform: Independent

Symptom: When you enter "ls /opsw/Server/@/m221.qa/files/arnold” on the managed server "m221.qa”, where the login account “arnold” is disabled, Opsware Global Shell displays an “RFS specific error”.

Workaround: Enable the login account on the managed server or revoke permissions to access the managed server using that account.

Bug ID: 30597

Description: When sequence-prepend is specified, outer scope sequence values are used even though Block Inheritance is specified.

Platform: Platform Independent

Subsystem: OCC Client - Application Configuration

Symptom: When Block-inheritance is specified on a sequence that is set to sequence-prepend, it is incorrectly blocking the inner scope values instead of the

outer scope values. Thus, it is possible to end up with values from the outer scope, instead of the inner scope in the merged sequence.

For example:

```
CML file
=========
@!filename-key="/test/file"@
@!filename-default="/tmp/file"@
@!namespace=/test/preserveValuesWithExplicitNull/@
@!sequence-prepend@
set1=@set1;unordered-string-set@



Server Scope Values
===================
set1/1=a
set1/2=b
set1/3=c
Server Instance Scope Values
============================
set1/1=Block Inheritance
set1/2=1
set1/3=2
Preview Output
==============
set1=a b c
```

Workaround: Use sequence-append.

Packages

Bug ID: 27021

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

Platform: Windows

Subsystem: Packages

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

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

Patch Management

Bug ID: 22960

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

Platform: Windows

Subsystem: Patches

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

Workaround: None.

Bug ID: 28871

Description: Opsware SAS 5.2 does not support MBSA version 2.0 for patch management.

Platform: Windows

Subsystem: Patch Management

Symptom: During the installation of Opsware SAS, you are required to upload the mbsacli.exe patch utility, which is shipped with the Microsoft Base Security Analyzer (MBSA version 1.2.1). Although MBSA version 2.0 is available from Microsoft, Opsware SAS 5.2 does not support MBSA version 2.0 for patch management.

Workaround: None. Do not upload MBSA version 2.0, since Opsware does not support MBSA version 2.0 for patch management.

Satellite

Bug ID: 27982

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

Platform: Platform Independent

Subsystem: Software Repository Cache

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

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

Software Provisioning

Bug ID: 26956

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

Platform: Platform Independent

Subsystem: Templates

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

Workaround: None.

Web Services Data Access Engine

Bug ID: 28568

Description: Error occurs in the Web Services Data Access Engine log file when you access the Manage Sever page.

Platform: Platform Independent

Subsystem: Web Services Data Access Engine

Symptom: In the Opsware Command Center when you access the Manage Sever page for the first time, a benign exception occurs in the Web Services Data Access Engine log file.

Workaround: None.

Bug ID: 30504

Description: A user with read-only permission to a specific customer and to all node stacks can associate the customer with a node.

Subsystem: Core - Web Services Data Access Engine

Platform: Independent

Symptom: In the WS API, the user can successfully associate the customer with the setCustomers operation of the Node Web Service. The user can also successfully invoke the detachCustomers operation. Although the user does not have the necessary read-write permissions, an OpswareAccessControlException is not thrown.

Workaround: None

Miscellaneous

Bug ID: 28809

Description: Patch uninstallation fails with errors.

Subsystem: Reconcile Backend

Platform: Solaris

Symptom: In Solaris 10, when you uninstall any patch, the uninstallation fails with the following error:

```
Backout of another patch is in progress try after some
time.
```

This error can occur because the server you are attempting to uninstall a patch from does not have the Solaris 10 patch 119254-06 installed on it.

Workaround: Install patch 119254-06 for Solaris 10. Without patch 119254-06, uninstalling patches on Solaris 10 servers will experience intermittent failures and display an error on the managed server.

Bug ID: 29058

Description: Duplicate server IDs specified for the addServers operation of the ServerGroup Web Service are not ignored.

Subsystem: Server Groups Backend

Platform: Independent

Symptom: When the addServers operation is invoked, if the list of server IDs contains duplicates, the operation fails and throws an OpswareException. This behavior also occurs with the setServers, removeServers, and moveServers operations.

Workaround: Do not specify duplicate server IDs.

Documentation Errata

Updates to the Opsware SAS 5.3 User's Guide

The followings topics in the Opsware SAS 5.3 User's Guide are updated with new information.

Managing Custom Attributes

The section "Managing Custom Attributes" section in the Opsware SAS User's guide is updated to include the following information:

When you add or edit server custom attributes using the Opsware Command Center, Opsware SAS removes leading and trailing whitespace characters from custom attribute values.

Opsware Global File System (OGFS)

The section "Opsware global File System (OGFS)" section in the Opsware SAS User's guide is updated to include the following information:

When you add or edit server custom attributes in the Opsware Global File System (using Global Shell), Opsware SAS preserves leading and trailing whitespace characters in custom attribute values.

Server Objects

The section "Server Objects" section in the Opsware SAS User's guide is updated to include the following information:

A Windows COM category (folder) that does not have any objects will not be included in a snapshot or audit, even though Opsware SAS will display an empty COM folder in the Server Explorer. A snapshot or audit will include a Windows COM category when it includes at least one object.

Setting Up Snapshot Selection Criteria

The section “Setting Up Snapshot Selection Criteria” section in the Opsware SAS User’s guide is updated to include the following information:

In the Selection Criteria Editor you can select a Windows COM category (folder) whether it contains objects or not. The Selection Criteria Editor and the Server Explorer display all Windows COM folders, whether they are empty or not.

Browsing Contents of a Snapshot

The section “Browsing Contents of a Snapshot” section in the Opsware SAS User’s guide is updated to include the following information:

Opsware SAS provides warning messages that explain how Windows COM folders were processed. The following scenarios apply:

• When you create a snapshot where you selected a Windows COM folder that does not contain any objects, the Snapshot Browser displays a summary. Opsware SAS displays a warning that the GUID (Globally Unique Identifier) for that folder is invalid, which means that the Windows COM folder does not contain any objects.

• When you create a snapshot where you selected a Windows COM object that does not exist on a target, Opsware SAS displays a warning that the folder is invalid.

• When you create a snapshot where you selected a Windows COM folder that does not contain any objects and a Windows COM folder that does contain objects, the Snapshot Browser displays the folder. Opsware SAS displays a warning that the folder is empty.

Overview of Custom Fields for Servers

The section “Overview of Custom Fields for Servers” section in the Opsware SAS User’s guide is updated to include the following information:

In order for the custom fields to appear in the Manage Server: Properties page, you will have to initially create a custom field. To create a custom field, you will need to install the custFields.py Custom Extension which is available only from the Content

Starter Pack. Contact your Opsware Technical Support for assistance in installing the custFields.py Custom Extension in Opsware SAS.

Application Configuration "Block Inheritance" - Additional Note

The section “Using Application Configuration Management” in the User’s Guide is updated to include this additional note for the Block Inheritance feature:
To block a namespace sequence from inheriting from other scopes, you should add a new namespace sequence that has the a single scalar value or the only entry in a sequence set to <Block Inheritance> with all other fields empty.

Updates to the Opsware SAS 5.3 Administration Guide

The following topic in the Opsware SAS 5.3 Administration Guide is updated with new information.

Web Services Data Access Engine Logs

The Web Services Data Access Engine contains the following log files:

```
var/lc/twist/stdout.log*
/var/lc/twist/twist.log
/var/lc/twist/access.log
/var/lc/twist/server.log*
/var/lc/twist/boot.log
/var/lc/twist/watchdog.log
```

The `stdout.log` file contains debug output and logging of every exception that the server generates. The file does not conform to a specific format. * indicates the files are 1og.1, log.2, log.3, and so forth. The number of files and the size of each file can both be configured via twist.conf. Additional logs are created when the specified maximum file size is reached. stdout.log is the most recent, and stdout.log.1 through 5 are progressively older files. The file is also rotated on startup.

This file also contains the output of any System.out.println(), System.err.println() and e.printStackTrace() statements.

The `twist.log` file contains JBoss-specific error or informational messages and Weblogic specific messages. These files are rotated on startup.

The `access.log` file contains access information in common log format. These files are rotated when the file reaches 5MB in size.

The server.log file contains debug messages generated from the Web Services Data Access Engine. The debug messages are controlled by the log level set at the package or class level in the twist.conf file. * indicates the files are 1og.1, log.2, log.3, and so forth. The number of files and the size of each file can both be configured via twist.conf. The server.log.0 is always the current file, while server.log.9 is the oldest.

The boot.log file contains information on the initial stdout and stderr messages generated when the Web Services Data Access engine starts In addition, the boot.log file contains the output from Kill –QUIT commands.

The watchdog.log file records the status of the Web Services Data Access Engine once every minute.

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.