Opsware® SAS 5.2

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 5.2

Opsware SAS 5.2 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 5.2 includes the following new features:

- OS Provisioning Support in Opsware Satellites
- New Operations in Opsware SAS Web Services API 2.2
- Configuring Password Policy Parameters
- New Features in Opsware Data Center Intelligence (DCI) 1.6
- New Features in Opsware SAS DCML Exchange Tool (DET) 2.1
- Support For New Platforms in Opsware SAS 5.2
- Automated Upgrade to Opsware SAS 5.2

What's New In Opsware SAS 5.2

OS Provisioning Support in Opsware Satellites

With the Opsware Installer, you can install the OS Provisioning Boot Server and Media Server components in an Opsware Satellite. These components enable you to provision operating systems onto managed servers that are in the Opsware Satellite.

See “Opsware Satellite Installation” in the *Opsware SAS 5.2 Deployment and Installation Guide* for more information

New Operations in Opsware SAS Web Services API 2.2

The new operations in the Distributed Script web service enable the programmatic creation, retrieval, update, and deletion of scripts.

See the *Opsware SAS Web Services API 2.2 Guide* for more information.

Configuring Password Policy Parameters

In Opsware SAS 5.2, the Opsware administrator can enable and configure password policy parameters for accessing the Opsware Command Center. The passwords will be checked against the configured parameters when user accounts are created by the Opsware administrator or when passwords are changed by the users or the administrator. Users, including the administrators, will be alerted with an error message if their password does not match the criteria specified in the configured password policy parameters.

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

- Enable password policy features in the Opsware Command Center.

- Set the maximum number of consecutive repeating characters allowed for a password.
- Set the minimum character limit required for a password.
- Set the minimum non-alphabetic character limit required for a password.

The Opsware administrator can configure any number of the above mentioned password policy parameters for accessing the Opsware Command Center. See "Overview of Password Policy Parameters" in the *Opsware SAS 5.2 Configuration Guide* for more information.

New Features in Opsware Data Center Intelligence (DCI) 1.6

Opsware Data Center Intelligence (DCI) 1.6 release provides new features, enhancements, and several bug fixes. This release's new features include:

- A new Compliance Summary report
- A new "Policy Compliance Details " report window for both the Compliance Dashboard and Compliance Summary that provides categorized compliance summaries for individual servers
- An improved report chooser user interface designed for ease of use
- First-time global defaults for all report parameters upon installation and user-saved defaults report parameters
- Enhanced performance for generating reports
- Several bug fixes

See the *Opsware Data Center Intelligence (DCI) 1.6 Administrator's Guide* for more information.

New Features in Opsware SAS DCML Exchange Tool (DET) 2.1

DET 2.1 supports import and export of the following content the Opsware SAS 5.2 release:

- Custom Field Schema

- Server Groups
- User Groups
- Customers
- Packages

See the *Opsware SAS DCML Exchange Tool (DET) 2.1 Reference Guide* for more information.

Support for New Platforms in Opsware SAS 5.2

Opsware SAS 5.2 now supports the following operating systems for Opsware Agents:

- Solaris 10 on SPARC
- Red Hat Linux 4 AS (32 bit and 64 bit)
- Red Hat Linux 4 ES (32 bit and 64 bit)
- Red Hat Linux 4 WS (32 bit and 64 bit)

Opsware SAS 5.2 now supports the OS Provisioning for the following operating systems:

- Solaris 10 on SPARC
- Red Hat Linux 4 AS
- Red Hat Linux 4 ES

Automated Upgrade to Opsware SAS 5.2

In Opsware SAS 5.2, you can upgrade your Opsware installation to this release.

Opsware SAS 5.2 supports the following upgrade paths:

- Upgrading a Standalone Core from 4.8 to 5.2
- Upgrading a Multimaster Mesh from 4.8 to 5.2
- Upgrading Opsware Satellites from 4.8 to 5.2
- Upgrading a Standalone Core from 5.1 to 5.2

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

Contact your Opsware Support Representative for information about upgrading to Opsware SAS 5.2.

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 5.2 supports. For complete information on package types and file types, see Chapter "Package Management" in the *Opsware SAS 5.2 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)	Depot	.tar
	Product	N/A
	Fileset	N/A
	Patch Product	N/A
	Patch File	N/A

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

Supported Browsers

The Opsware SAS 5.2 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 8 (on SPARC) Solaris 9 (on SPARC)
Red Hat Linux	Red Hat Enterprise Linux 2.1AS (32 bit) Red Hat Enterprise Linux 3AS (32 bit)

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

Supported Installations

The Opsware SAS 5.2 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 5.2 or Opsware SAS 5.1 to Opsware SAS 5.2. Refer to the *Opsware SAS 5.2 Upgrade Guide* for more information.

Documentation

This release comes with the following documentation:

- *Opsware SAS 5.2 Release Notes*
- *Planning Deployments for Opsware SAS 5.2*
- *Opsware SAS 5.2 Deployment and Installation Guide*
- *Opsware SAS 5.2 Configuration Guide*
- *Opsware SAS 5.2 Administration Guide*
- *Opsware SAS 5.2 User's Guide*
- *Opsware Data Center Intelligence 1.6 Administrator's Guide*
- *Opsware DCI 1.6 Release Notes*
- *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 5.2*

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

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 are for Opsware SAS 5.2 compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 5.2 features with Opsware Agent versions prior to 5.2 yielded the following results for the new features in the Opsware Command Center and the OCC Client.

Opsware Command Center Features

The following new Opsware Command Center features are compatible with Opsware Agents 4.5 and later:

- Server Search
- Server Groups
- Custom Fields

However in Opsware SAS 5.1 and 5.2, the functionality of the Agent increased so that Agent hardware registration with an Opsware core returns additional server attributes. When you search for Opsware Agents using these attributes, the search results will not include servers running servers running Opsware Agents prior to 5.2.

OCC Client Features

The following new 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

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

What's Fixed in Opsware SAS 5.2

The following bugs have a severity level of Critical or Major and are fixed in Opsware SAS 5.2.

Access and Authentication

Bug ID: 27800

Description: When you created a user group, with the string CDR, or CDS, or CDT in the group name, the newly created group would not be in the group list, and when you tried to create the same group again, the operation failed with an error.

Platform: Platform Independent

Subsystem: Users and Groups

Resolution: Fixed.

Installer

Bug ID: 28717

Description: The Opsware Installer prompts for the facility name during the interview for adding a core to a mulitmaster mesh. If you enter a facility name that contains spaces, the characters after the first space are lost. (For example, "Sunnyvale Center" becomes "Sunnyvale." The Oracle TNSNAME and the Opsware Multimaster listener fail.

Platform: Independent

Subsystem: Installer

Resolution: Fixed. You can specify a facility name that contains one or more spaces.

Packages

Bug ID: 28064

Description: In Solaris and Windows, when you uploaded the following packages from the Packages page, a null pointer exception occurred.

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

This behavior was only observed in the following cases:

- If you used FireFox browser to access the Opsware Command Center.
- If you set the customer filter to "All Customers" before you uploaded the packages.

Platform: Solaris and Windows

Subsystem: Packages

Resolution: Fixed. You can use FireFox browser to upload packages from the Opsware Command Center.

Opsware Agent

Bug ID: 27360

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

Platform: Windows

Subsystem: Agent

Resolution: Fixed.

Bug ID: 27530

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

Platform: Platform Independent

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

Resolution: This has been fixed.

Bug ID: 29022

Description: Upgrading the Opsware Agent resets the Windows registry settings for Python 1.5 to Opsware specified values.

Platform: Windows

Subsystem: Agent Upgrade Tool

Resolution: Fixed. The Agent Upgrade Tool (opsh) now checks the Windows registry settings for Python 1.5 before upgrading the Agent. If they are not as expected, opsh will skip upgrading the Agent with the message "Found a Python1.5 installation which was not installed by the Opsware agent."

OCLI

Bug ID: 2979

Description: opswrapper.Template.new () did not work when the recurse parameter was set to 1.

Platform: Independent

Subsystem: OCLI

Workaround: This has been fixed.

Opsware Command Center

Bug ID: 28864

Description: In the OCC when you add a node to a Software Tree, you can check the “Allow Servers” check box to assign servers to that node. In Opsware SAS 5.1, even if you did not check the “Allow Servers” checkbox, the allow servers flag was being set allowing for servers to be assigned to the node.

Platform: Independent

Subsystem: Software Provisioning

Resolution: This has been fixed in Opsware SAS 5.2.

OCC Client

Bug ID: 26121

Description: The audit progress bar displayed that the process was 100% complete when it was still taking snapshots of targets.

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Resolution: Fixed. Progress information was not being processed correctly.

Bug ID: 27073

Description: Audit results were incorrect when you re-ran the same audit after performing a Copy To. You audited the file system of two live servers that were running SunOS5.9. In the Audit Result Browser, you saw that a file existed Only on Source. You used the Copy To action to copy a file to the target server. When you re-ran the same audit, the results displayed the same differences with one less difference Only on Source and one more difference On Both But Different. When you viewed the results that are On Both But Different, you did not see the copied file as the difference. Instead, that file's parent directory was listed as the difference, which was misleading. For example, before the Copy To, the file was ID 1060666. After you used the Copy To action and after you re-ran the audit, the audit results referred to this file as ID 1070666.

Platform: Platform Independent

Subsystem: OCC Client - Audit & Compliance

Resolution: Fixed. Modified unzip to preserve the time stamps on directories when extracting files or creating subdirectories. However, if you are using Opsware SAS 5.1 Agents with an Opsware SAS 5.2 core, this problem is not fixed.

Bug ID: 27750

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

Platform: Platform Independent

Subsystem: OCC Client – Audit & Compliance

Resolution: Fixed. The audit result did not verify whether the SID object existed.

Bug ID: 27833

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

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Resolution: Fixed. To use Visual Packager to create Windows 2000 or Windows 2003 packages and upload them to the Software Repository, you do not need the Packages user permission in Opsware SAS.

Bug ID: 28032

Description: Preview differences on imported values for Application Configuration. When you created an application configuration using the Import Value function and performed a preview for the first time (i.e., the values had not yet been pushed to the server), you would see differences in the preview due to the way the CML parser handled comments in the source configuration file. Once you pushed the application configuration to a server, the preview differences would no longer show (unless other changes were made).

Platform: Platform Independent

Subsystem: OCC Client - Application Configuration Management

Resolution: This has been fixed. Now preview differences for applications configurations that were imported are shown before and after the changed are pushed to the server.

Bug ID: 28754

Description: When you used Visual Packager to create a package based on a snapshot or an audit result, some file system content that was in first-level subdirectories and below was not included in the package. For example, you tried to create a package (using a snapshot or an audit as the source) that contained the following file system content:

```
c:\temp.txt
c:\dir\ (All content under c:\dir\ was selected for
packaging.)
c:\dir\ file1.txt
c:\dir\file2.txt
c:\dir\subdir\
```

Only the c:\temp.txt file was included in the package. The remaining file system content was not included in the package.

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Resolution: Fixed. Visual Packager can now create a package (based on a snapshot or an audit result) that contains file system content in first-level subdirectories and below.

Opsware Gateway

Bug ID: 28954

Description: In the Opsware Gateway properties file, if the opswgw.ForwardUDP entry includes the optional IP address, the UDP forward does not work.

Platform: Independent

Subsystem: Opsware Gateway

Resolution: Fixed. You can specify the IP address in opswgw.ForwardUDP. For the syntax of the properties file, see Appendix C in the Opsware SAS 5.2 Deployment and Installation Guide.

Web Services

Bug ID: 27676

Description: A Distributed Script Execution (DSE) script cannot be uploaded with the Web Services API.

Platform: Platform Independent

Subsystem: Web Services

Resolution: Fixed. The following operations have been added to the Distributed Script Web Service and have been documented in the Web Services API 2.2 Guide:

```
get
 getCurrentVersion
 getScriptText
 create
 update
 updateScriptText
 delete'
```

Bug ID: 27885

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

Platform: Platform Independent

Subsystem: Web Services

Resolution: This has been fixed.

Known Problems, Restrictions, and Workarounds in Opsware SAS 5.2

This section describes the workarounds to known problems in Opsware SAS 5.2.

Access and Authentication

Bug ID: 23457

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

Platform: Platform Independent

Subsystem: Access and Authentication

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

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

Bug ID: 27675

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

Platform: Platform Independent

Subsystem: Access and Authentication

Symptom: If the external LDAP server is configured to require client certificates, then the Opsware 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).

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.

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.

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: 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.

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

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”.

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: 29162

Description: New Facilities or Customers is not displayed in the Opsware Command Center.

Subsystem: Opsware Command Center

Platform: Independent

Symptom: When a new Facility or Customer is created in an upgraded Opsware SAS 5.2 core (upgraded from Opsware SAS 4.8), the Facility or Customer does not show up in the OCC. This behavior is only observed when the Web Services Date Access Engine is not responding or running when you launch the OCC. As a result, the objects in the ACDCCacheRegistrar which includes the Facilities and Customers are not updated when the Web Services Date Access Engine restarts.

Workaround: Wait for the Web Services Date Access Engine to restart and then restart the Opsware Command Center.

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.

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: 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: 29039

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

```
NameError: display_warning
```

This means that the files with unknown users and user groups will not have their information set. Because this is a warning, the snapshot process does succeed.

Platform: Platform Independent

Subsystem: OCC Client - Audit & Compliance

Symptom: You try to create a snapshot of files that are owned by unknown users or user groups and receive a warning message.

Workaround: None.

Bug ID: 29046

Description: The creating a package process fails when you select two operating systems (where one operating system is Redhat AS4) or when you select one packaging server that is Redhat AS4.

Platform: Platform Independent

Subsystem: OCC Client - Visual Packager

Symptom: You launch Visual Packager from a packaging server that is a Redhat AS4 operating system. Select files and packages and try to create a package. The packaging process fails.

Workaround: None.

Bug ID: 29051

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

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Symptom: In the Details tab of the Create Package window, select a package in the Installed Packages list. In the "Packages that exist in the software repository" section in the Contents tab, select a new file to replace (overwrite) the package. During package creation, you get a

Database Unique Constraint Error.

Workaround: To replace (overwrite) an existing package, use the OCC to re-upload the package.

Bug ID: 29053

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

Platform: Platform Independent

Subsystem: OCC Client – Visual Packager

Symptom: In the Create Package window, one of the categories (such as File System or Installed Patches) includes only one item. Select another item for that same category (that has the single item) and then go to the Contents tab to see all selections displayed. Go to the Details tab and remove the category that has one item (deselect that one item). Go back to the Contents tab to see that the other item is not displayed and that the category contains no items.

Workaround: Do not deselect an item after you have made a selection. If you make this mistake, close the Create Package window and start over.

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: 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

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.

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 assigned to the customer associated with the template.
When you create a template that is Customer Independent, select the No option in the Assign Customer field.

Workaround: None.

Web Services Data Access Engine

Bug ID: 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.

Miscellaneous

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.

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.

Documentation Errata

Updates to the Opsware SAS 5.2 Configuration Guide

The following topics in *Opsware SAS 5.2 Configuration Guide* are updated with new information.

OS Provisioning Setup

The chapter OS Provisioning Setup in the *Opsware SAS 5.2 Configuration Guide* is updated to include the following information:

To provision Fujitsu Solaris systems, use the appropriate media. For Fujitsu Solaris 8, use the Solaris 8 media supplied by Fujitsu, including the appropriate patches. (These patches are installed as a build customization before the reboot or they can be placed in the patches subdirectory of the operating system media.) For Fujitsu Solaris 9, use the Solaris 9 media from one of the later hardware releases. For Fujitsu Solaris 10, use the normal Solaris 10 media.

Using an External LDAP Directory Server with Opsware SAS

To configure an external LDAP for authentication with Opsware SAS, one of the steps is to add aaa.ldap entries to the Web Services Data Access Engine (twist) configuration file. Instructions for modifying this file are in the section "Using an External LDAP Directory Server with Opsware SAS" in the *Opsware SAS 5.2 Configuration Guide*.

In this release, this section incorrectly instructs you to edit the twist.conf file. The correct file to edit is /cust/twist/etc/twistOverrides.conf. This file will be preserved during Opsware SAS upgrades.

ZIP Package Support

The section “ZIP Package Support” in the *Opsware SAS 5.2 Configuration Guide* is updated to include the following information:

The Opsware Command Center supports ZIP packages on Windows 2003.

Updates to the Opsware SAS 5.2 Deployment and Installation Guide

The following topics in *Opsware SAS 5.2 Deployment and Installation Guide* are updated with new information.

Oracle Setup for Model Repository

In the printed version of the *Opsware SAS 5.2 Deployment and Installation Guide*, the "Oracle Setup for Model Repository" appendix has some out of date information on recommended tablespace sizes and init.ora parameters. For the latest information, see the PDF version of the guide on our web site.

Steps for Adding a Core to a Multimaster Mesh

The section “Steps for Adding a Core to a Multimaster Mesh” in the *Opsware SAS 5.2 Deployment and Installation Guide* is updated to include the following information:

If you are adding a third (or more) core to a multimaster mesh, you can export data from a core other than the original source (master) core. (In the instructions that follow, the core that you will export data from is referred to as core #2.) If you decide to take this approach, then you must perform the following steps:

a) On the source core, define a new facility.

(See step 11 in "Steps for Adding a Core to a Multimaster Mesh.")

b) Wait for the transactions to propagate to core #2 before performing the export.

c) Export the data from core #2.

(See step 17 in "Steps for Adding a Core to a Multimaster Mesh.")

By default, the new target core will try to connect to the source (master) core. If you want the new target core to connect to core #2 instead of the source core, then you must configure TIBCO manually and edit the Opsware Gateway properties file. For instructions, see the section "Adding a TIBCO Rendezvous Neighbor" in the *Opsware SAS 5.2 Deployment and Installation Guide.*

Windows Deployment Agent Helper

The PDF version, the section “Windows Deployment Agent Helper" in the *Opsware SAS 5.2 Deployment and Installation Guide* has been updated to include an additional step. For the latest information, see the PDF version of the guide on our web site.

Open Port 8081 Required for ODAD

The section “Open Port 8081 Required for ODAD“ in the Opsware SAS 5.2 Deployment and Installation Guide is updated to include the following information:

In addition to the open ports documented in the Opsware SAS 5.2 Deployment and Installation, port 8081 must also be open on the servers running core or Satellite Gateways. Port 8081 is needed for the ODAD feature.

Updates to the Opsware SAS 5.2 User’s Guide

The following topics in *Opsware SAS 5.2 User’s Guide* are updated with new information.

Windows OS Provisioning

The section “Windows OS Provisioning” in the *Opsware SAS 5.2 User’s Guide* does not list Windows 2003 as a supported platform for OS Provisioning. Opsware supports OS Provisioning on Windows 2003.

Updates to the Opsware SAS 5.2 Administration Guide

The following topic in *Opsware SAS 5.2 Administration Guide* is updated with new information.

Multimaster Central Data Access Engine

The information in the topic "Designating the Multimaster Central Data Access Engine" in Chapter 4, is replaced with the following information.

The Opsware Installer automatically assigns the multimaster central Data Access Engine when you install an Opsware core.

Opsware Inc. recommends that you do **not** change this designation post-installation. Designating another Data Access Engine in the multimaster mesh the multimaster central Data Access Engine can affect your ability to upgrade an Opsware SAS core to the latest version.

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.