Opsware® SAS 6.61 Release Notes

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.
T + 1 408.744.7300 F +1 408.744.7383 www.opsware.com

Table of Contents

Chapter 1: New in Opsware SAS 6.61

IN THIS CHAPTER

This chapter contains the following topics:

- Rolling Mesh Upgrades (SAS 6.6 to 6.61 only)
- Windows 2003 64-bit Native Agent
- Remediation and the AIX Logical Volume Manager (LVM)
- Aix Patching Support Improvements
- SAS Client Installer (v.1.2)
- Critical Bug Fixes

Opsware Server Automation System (SAS) 6.61 automates critical areas of server and application operations – including the provisioning, patching, server and application configuration change management, compliance checking and reporting – across major operating systems and a wide range of software infrastructure and applications.

The following sections describe all new features and enhancements in the Opsware SAS 6.61 release.

Rolling Mesh Upgrades (SAS 6.6 to 6.61 only)

SAS 6.61 supports Rolling Mesh (or mesh up) upgrades from SAS 6.6 through the use of tunneled connections between Core Gateways and Agent and Satellite gateways that allow management of a core's servers to be taken over by other cores while it is down for upgrade. For more information about Rolling Mesh Upgrades, see the *Opsware® SAS 6.61 Upgrade Guide*.

Windows 2003 64-bit Native Agent

Windows 2003 64-bit native agents are now supported.

Remediation and the AIX Logical Volume Manager (LVM)

The AIX Logical Volume Manager (LVM) can now be to temporarily set up a file system for staging file sets that will be installed during reconciliation.

An AIX administrator can set aside unused disk space, diskspace that is part of a volume group but that is not allocated to any mounted file system. Using the AIX VM, it is trivial to create a temporary file system, on-the-fly, that uses this unused space. When the need for the temporary files system is done, it can be destroyed, freeing the disk space.

After the AIX administrator provides the volume group by specifying a custom attribute, SAS can then determine how much space it needs to stage any file sets to be installed, create a temporary file system for these filesets, then after installing the file sets, destroy the temporary file system.

For more information about AIX patching support improvements, see the *Technical Note: AIX Patching*.

Aix Patching Support Improvements

For more information about AIX patching support improvements, see the *Technical Note: AIX Patching Support*.

SAS Client Installer (v.1.2)

As of SAS 6.61, the SAS Client Launcher is version 1.2.

The launcher has a new *Advanced Setting* option where you can specify proxy settings as well as delete the application cache/logs.

The SAS Client Launcher is independent of the SAS Client versions, therefore, it can be used to connect to and launch all SAS 6.5 and later SAS Clients.

Critical Bug Fixes

The following critical issues have been addressed and fixed in 6.61:

Table 1-1: Fixed Critical Bugs

BUG NUMBER	DESCRIPTION
144339	SAS/NAS integration memory leak
151807	Agent does not have full access to 'c:\windows\system32' on 64 bit windows
157409	Patch uninstallation job for APAR is completed but status of APAR uninstall is **Pending**
159502	OGSH sessions not closing on timeouts
160494	Waybot is not handling failure to start PENDING jobs during startup properly
160917	Uncaught exceptions in `cogscript_ng`
161147	DET Filter Editor [GUI] - Import of filter fails when there is an entry of Custom Fields Schema Filter
161205/ 161206	`tzupdater` for `tzdata2007k` is available
161227	OCC runs out of memory
161495	`java.lang.NullPointerException`: No patches imported when one of multiple selected patches does not have a specified URL
161500	`ismtool` throws an exception when invoked on Windows 2003 x86_64
161577	Interleaving can cause RPM upgrades to fail if installed RPMs require same versions of other installed RPMs
161596	Memory leak in `cogscript_ng` way script
161599	Memory leak in `check_reachability`
161674	Snapshot Cache Manager makes unnecessary snapshot copies
161676	AppConfig push timeout is not calculated correctly

Chapter 2: Platform and Environmental Support

IN THIS CHAPTER

This chapter contains the following topics:

- Supported Operating Systems
- Supported Core Operating Systems
- Operating System Deprecation and End of SupportOperating System Deprecation and End of Support
- Supported Installations and Upgrades for Opsware SAS 6.61
- SAS Client Java Version
- Documentation for Opsware SAS 6.61

Supported Operating Systems

This section lists the supported operating systems for Opsware Agents and the SAS Client.

Opsware Agents

The following table lists the supported operating systems for Opsware Agents, which run on the servers managed by Opsware SAS.

Table 2-1: Opsware Agent Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
AIX	AIX 4.3 AIX 5.1 AIX 5.2 AIX 5.3	POWER POWER POWER POWER

Table 2-1: Opsware Agent Supported Operating Systems (continued)

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
HP-UX	HP-UX 10.20 HP-UX 11.00 HP-UX 11.11 HP-UX 11.23 (11i v2) HP-UX 11iv3	PA-RISC PA-RISC PA-RISC PA-RISC and Itanium PA-RISC and Itanium
Sun Solaris	Solaris 6 Solaris 7 Solaris 8 Solaris 9 Solaris 10 (Update 1, Update 2, Update 3)	Sun SPARC Sun SPARC Sun SPARC Sun SPARC Sun SPARC, 64 bit x86, 32 bit x86 and Niagara
Fujitsu Solaris	Solaris 8 Solaris 9	Fujitsu SPARC Fujitsu SPARC
Windows	Windows NT 4.0 Windows 2000 Server (Service Pack 4 or higher) Windows Server 2003 Windows XP Professional	32 bit x86 32 bit x86 32 bit x86 and 64 bit x86 32 bit x86

Table 2-1: Opsware Agent Supported Operating Systems (continued)

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
Red Hat Linux	Red Hat Linux 7.3	32 bit x86
	Red Hat Linux 8.0	32 bit x86
	Red Hat Enterprise Linux 2.1 AS	32 bit x86
	Red Hat Enterprise Linux 2.1 ES	32 bit x86
	Red Hat Enterprise Linux 2.1 WS	32 bit x86
	Red Hat Enterprise Linux 3 AS	32 bit x86 and 64 bit x86 and Itanium
	Red Hat Enterprise Linux 3 ES	32 bit x86 and 64 bit x86 and Itanium
	Red Hat Enterprise Linux 3 WS	32 bit x86 and 64 bit x86 and Itanium
	Red Hat Enterprise Linux 4 AS	32 bit x86 and 64 bit x86
	Red Hat Enterprise Linux 4 ES	32 bit x86 and 64 bit x86
	Red Hat Enterprise Linux 4WS	32 bit x86 and 64 bit x86
	Red Hat Enterprise Linux Server 5	32 bit x86 and 64 bit x86
	Red Hat Enterprise Linux Desktop 5	32 bit x86 and 64 bit x86
SUSE Linux	SUSE Linux Enterprise Server 8	32 bit x86
	SUSE Linux Standard Server 8	32 bit x86
	SUSE Linux Enterprise Server 9	32 bit x86 and 64 bit x86
	SUSE Linux Enterprise Server 10	32 bit x86 and 64 bit x86
VMware	ESX Server 3.0	32 bit x86 and 64 bit x86
	ESX Server 3.0.1	32 bit x86 and 64 bit x86
	ESX Server 3.0.2	32 bit x86 and 64 bit x86

On Red Hat Enterprise Linux 4 AS and 5, Opsware does not support SELinux (Security Enhanced Linux). By default, SELinux is enabled on Red Hat 4 AS and Enterprise Linux 5. You must disable the SELinux feature on Red Hat 4 AS and Enterprise Linux 5 for the Opsware Agent to function correctly.

Opsware SAS Client

The following table lists the operating systems supported for the SAS Client.

Table 2-2: SAS Client Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR SAS CLIENT	VERSIONS	ARCHITECTURE
Windows	Windows Vista	32 bit x86 and 64 bit x86
	Windows XP	32 bit x86
	Windows 2003	32 bit x86
	Windows 2000	32 bit x86

Supported Core Operating Systems

Table 2-3 lists the supported operating systems for Opsware Core Components.

For a list of supported Oracle versions for the Model Repository, see Appendix A in the *Opsware® SAS Planning and Installation Guide*.

Table 2-3: Opsware Core Supported Operating Systems

SUPPORTED OS FOR OPSWARE CORE	VERSIONS	ARCHITECTURE	OPSWARE COMPONENTS
Sun Solaris	Solaris 9	Sun SPARC	All components
Sun Solaris	Solaris 10	Sun SPARC, Niagara	All components
Red Hat Linux	Red Hat Enterprise Linux 3 AS	32 bit x86	All components
Red Hat Linux	Red Hat Enterprise Linux 4 AS	64 bit x86	All components

A guest OS (virtual machine) of a VMWare ESX server *is not supported* as an Opsware core server.

Table 2-4 lists the supported operating systems for Opsware Satellite Components:

- Gateway
- Software Repository Cache
- Boot Server (optional)
- Media Server (optional)

Table 2-4: Opsware Satellite Supported Operating Systems

SUPPORTED OS FOR OPSWARE SATELLITE	VERSIONS	ARCHITECTURE
Sun Solaris	Solaris 9	Sun SPARC
Sun Solaris	Solaris 10	Sun SPARC
Red Hat Linux	Red Hat Enterprise Linux 3 AS	32 bit x86
Red Hat Linux	Red Hat Enterprise Linux 4 AS	64 bit x86
SUSE Linux	SUSE Linux Enterprise Server 9	32 bit x86

Operating System Deprecation and End of Support

When a managed operating system is “end of life” by the operating system vendor, Opsware marks the operating system as deprecated as an indication that the operating system might be dropped from the list of supported managed operating systems in a future release of the SAS product.

Deprecated operating systems are supported in the current release of the product in the same way non-deprecated operating systems are.

Opsware monitors operating systems usage by its customers on an ongoing basis and bases the operating system retirement decisions on operating system usage by current customers.

If you have any questions related to the Opsware operating system deprecation policy, please contact Opsware support or your account manager.

The following operating system versions are being deprecated in Opsware SAS 6.61:

- Red Hat Linux 7.3

- Red Hat Linux 8.0

  (These operating systems have been deprecated since Opsware SAS 5.5.)

The following operating system versions are no longer supported in Opsware SAS 6.61:

- Red Hat Linux 6.2
- Red Hat Linux 7.1
- Red Hat Linux 7.2

  (These operating systems have been deprecated since Opsware SAS 5.5.)

Supported Installations and Upgrades for Opsware SAS 6.61

The Opsware SAS 6.61 release supports the following installations:

- Upgrading a standalone core from Opsware SAS 6.5.1.x and 6.6 to 6.61
- Upgrading a multimaster mesh from Opsware SAS 6.5.1.x and 6.6 to 6.61
- Upgrading an Opsware Satellite from Opsware SAS 6.5.1.x and 6.6 to 6.61

SAS Client Java Version

The SAS Client is installed with the Java™ 2 Runtime Environment, Standard Edition 1.4.2._15.

Documentation for Opsware SAS 6.61

This release comes with the following documentation:

- *Opsware SAS 6.61 Release Notes*
- *Opsware SAS 6.61 Upgrade Guide*
- *Technical Note: SAS AIX Patching Support*

The following documentation is applicable to this release:

- *Opsware SAS 6.6 Planning and Installation Guide*
- *Opsware SAS 6.5 Policy Setter's Guide*

- *Opsware SAS 6.5 Administration Guide*
- *Opsware SAS 6.5 User's Guide: Server Automation*
- *Opsware SAS 6.5 User's Guide: Application Automation*
- *Opsware SAS 6.5 Oracle Setup for the Model Repository*
- *Opsware SAS 6.5 Content Utilities Guide*
- *Opsware SAS 6.5 Content Migration Guide*
- *Opsware Automation Platform Developer's Guide*
- *SAS 3rd Party and Open Source Notices*

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 web site.

Chapter 3: Opsware Agent Compatibility

IN THIS CHAPTER

This chapter contains the following topic:

- Opsware Agent Compatibility

Opsware Agent Compatibility

The majority of the Opsware SAS Web Client features for Opsware SAS *6.61* are compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 6.61 features with Opsware Agent versions prior to 6.61 yielded the following results for the features in the Opsware SAS Client:

SAS Client Features – Agent Compatibility

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

- Application Configuration Management
- Server Browser
- Global Shell
- Audit and Remediation
- Visual Application Manager

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

The following features in the SAS Client are compatible with Opsware Agents 4.5 and later:

- Patch Management for Windows
- Patch Management for Unix

- Software Management

Windows multi-locale patching is only compatible on the Opsware Agent 5.5 or later.

Chapter 4: Fixed in Opsware SAS 6.61

IN THIS CHAPTER

This chapter contains bugs that have a severity level of Critical or Major and are fixed in Opsware SAS 6.61. These descriptions are arranged by the following features:

- AAA
- Agent Installer
- Agents
- Agent Upgrade
- Audit and Compliance
- Code Deployment and Rollback (CDR)
- Command Center (OCC)
- Command Engine
- Command-Line Interface
- Communication Test
- Data Access Engine
- DCML Export Tool (DET)
- DSE
- Gateways
- Global Filesystem (OGFS)
- Localization
- OS Provisioning
- Patch Management
- Reconcile
- Software Management

• Virtualization • Visual Analyzer • Visual Packager • Web Services Data Access Engine	

AAA

Bug ID: 161978

Description: Remote terminal case sensitive login problem.

Platform: Unix

Subsystem: Authentication, Authorization, and Accounting (AAA)

Symptom: A remote terminal session fails with the message `Press enter to close this Window` when the username invoking the remote terminal contains a capital letter.

Resolution: Fixed

Agent Installer

Bug ID: 159203

Description: Agent installation fails on managed servers that have Python 2.3 (SymphonyRPM) installed.

Platform: Windows

Subsystem: Agent Installer

Symptom: The Agent Installer fails on machines (Win2k/Win2k3) that have SymphonyRPM installed. Apparently, SymphonyRPM installs/uses Python 2.3.

Resolution: Fixed

Agents

Bug ID: 151807

Description: Agent does not have full access to `c:\windows\system32` on 64-bit Windows.

Platform: Windows Server 2003 x86_64

Subsystem: Agent

Symptom: File access to the System32 and subdirectories are transparently redirected based on the bitness of the process making that file access (64-bit processes have full access, while 32-bit processes have access to System32 redirected to Syswow64).

Syswow64, in turn, is missing 100 or so files, including `diskpart.exe`. Since the Agent's python binary is 32-bit, it cannot see `diskpart` and, hence, any DSE or post-install script that needs to call it will fail.

Resolution: Fixed

Bug ID: 160649

Description: HP-UX 11.23 in trusted mode not allowing remote session.

Platform: HP-UX 11.23

Subsystem: Agent

Symptom: An HP-UX server running in trusted mode does not allow a remote shell connection to be established. The system can be managed using SSH or telnet but the console cannot make a connection.

Resolution: Fixed

Bug ID: 161401

Description: `alt0` NIC on SunOS 5.8 not recognized by SAS.

Platform: SunOS 5.8

Subsystem: Agents

Symptom: `bs_hardware` does not recognize alt0 NIC on SunOS 5.8.

Resolution: Won't Fix

Bug ID: 161500

Description: The ismtool throws an exception when invoked on Windows 2003 x86_64.

Platform: Windows 2003 x86_64

Subsystem: Agent

Symptom: Remediate the ISMTool software policy from **Library ➤ By Type ➤ Software Policies ➤ Windows 2003 x64 ➤ Windows ISMTool** on a Windows 2003 x64 machine

On the Windows machine go to the folder:

```
C:\Program Files (x86)\ismtool-3.4.2\bin>
```

Run the command `ismtool.cmd.`

A popup windows appears with the error:

```
This application has failed to start because PyWinTypes15.dll
was not found. Re-installing the application may fix this error.
```

Resolution: Fixed

Bug ID: 161880

Description: RDP sessions on servers with more than one physical CPU might cause the agent to restart.

Platform: Windows

Subsystem: Agent

Symptom: RDP sessions to Windows servers might cause the agent to restart. The symptoms are:

In the event log you see the following entry:

```
The Opsware Agent exited and exit status was 3. The Agent will
be restarted.
The service is creating a process to run this command:
"C:\Program Files\Loudcloud\lcpython15\python.exe"
"C:\Program Files\Loudcloud\blackshadow\shadowbot\
shadowbot.pyc" --conf
"C:\Program Files\Common Files\Loudcloud\cogbot\
etc\cogbotservice.args" "
```

The Opsware Agent has been started.

In `OPSWshadowbotservice.out` you can see the following message:

```
Fatal Python error: ceval: tstate mix-up
```

followed by the usual messages printed when the agent starts up.

Finally, the RDP session dies.

Resolution: Fixed

Bug ID: 162256

Description: Under SAS 6.x Agent recertification fails when run on a Managed Server with a pre-SAS 6.x Agent.

Platform: Windows

Subsystem: Agent Deployment/Upgrade Backends

Symptom: Under SAS 6.x, in the SAS Client, if you select a Managed Server that is running a pre-SAS 6.x Agent and run the Custom Extension `Agent_Recert`, the recertification fails with the error:

```
The Agent encountered a fatal error when writing the crypto
material
```

Resolution: Fixed

Bug ID: 164924/124471

Description: Bonded interfaces on Linux aren't handled properly by `bs_hardware`, etc.

Platform: Independent

Subsystem: Agents

Symptom: Bonded interfaces aren't handled properly by `bs_hardware`. If the customer is using a bonded interface over multiple real interfaces, the bonded interface isn't visible, modifiable, and so on.

Resolution: Fixed

Bug ID: 165674

Description: Agent install failure: `vcredist` run failed.

Platform: Windows 2000

Subsystem: Agents

Symptom: Deploying SAS 6.62 Agents on Windows 2000 hosts, requires at minimum Service Pack 4 (SP4) be installed on the Windows 2000 host.

Resolution: Wontfix

Bug ID: 165703

Description: Agent's Windows interface detection – intermittent failure.

Platform: Windows

Subsystem: Agent

Symptom: When deploying a Storex Agent for asset discovery to a Windows host, Storex depends on SAS to detect interfaces, however, the Oracle database instance does not show up for Windows 2000 causing interface detection failures.

Resolution: Fixed

Agent Upgrade

Bug ID: 161788/163415

Description: Agent upgrade Fails with `KeyError: dvc_role_id`.

Platform: Windows

Subsystem: CX: Agent Upgrade

Symptom: While attempting to do an Agent upgrade by Running a Custom Extension, the Agent is not upgraded and you get a Command Engine Script Failure in the SAS Web Client.

Resolution: Fixed

Audit and Compliance

Bug ID: 165268

Description: IIS Metabase cannot be accessed from SAS.

Platform: Windows

Subsystem: Audit and Compliance Backend

Symptom: IIS Metabase isn't displayed in the Server Browser due a Windows NT bug.

Resolution: Won't Fix

Code Deployment and Rollback (CDR)

Bug ID: 162507

Description: Unacceptable performance of CDR DataAccess APIs.

Platform: Independent

Subsystem: Code Deployment and Rollback (CDR)

Symptom: Code Deployment and Rollback (CDR) was providing unacceptable performance levels due to inefficiencies in the implementation of the DataAccess APIs used by CDR.

Resolution: Fixed

Command Center (OCC)

Bug ID: 160333

Description: Custom Attributes attached to Device Groups truncate the value if quote character (`"`) is present.

Platform: Independent

Subsystem: Command Center (OCC) - Web: Servers

Symptom: When adding a Custom Attribute similar to the following:

```
PATCH 119059 31 31 "Xsun patch" (All_Products)
PATCH 120011 14 14 "kernel patch" (All_Products)
PATCH 119963 08 08 "C++ shared library Patch" (All_Products)
PATCH 120753 05 05 " Microtasking libraries Patch" (All_
Products)
```

the actual custom attribute stored is the following:

```
PATCH 119059 31 31 \
```

and nothing more after the “ \ “ character because the (`"`) character is not being handled correctly.

Resolution: Fixed

Bug ID: 161130

Description: Page numbers do not appear on window for attaching device groups to OCC groups.

Subsystem: Command Center (OCC) - Web: Servers

Platform: Independent

Symptom: In OCC, you are only able to see the first 500 device groups under a single node and page numbers for additional listings over 500 are unavailable.

Resolution: Fixed

Bug ID: 161169

Description: Editing a large inherited custom attribute corrupts the name of the custom attribute.

Subsystem: Command Center (OCC): Administration

Platform: Independent

Symptom: The name of a custom attribute could be displayed incorrectly after the attribute was edited due to HTML rendering issues.

Resolution: Fixed

Bug ID: 162718

Description: Custom attribute named `what` breaks handling of all custom attributes.

Subsystem: Command Center (OCC): Other/Misc.

Platform: Independent

Symptom: Open a managed server in the OCC web, go to **Custom Attributes**, click **New** and create a custom attribute with the name `what and` click **Save**. After creating this custom attribute, if you select **Edit**, **Delete**, or **Revert**, the page refreshes but nothing else happens.

Resolution: Fixed

Bug ID: 164608/161227

Description: Command center (OCC) memory settings are too low.

Subsystem: Command Center (OCC) Web: Software.

Platform: Independent

Symptom: OCC authentication fails due to an Out of Memory condition.

Resolution: Fixed

Command Engine

Bug ID: 154424/163701

Description: Unprovisioned Servers will not persist a list servers where the number of servers is a multiple of ten / Unprovisioned Servers List does Not Display Servers in the Server Pool.

Platform: Independent

Subsystem: Command Engine Client Framework

Symptom: Scenario:

Starting with an empty pool, add 50 servers to the server pool using a custom extension to generate 50 servers with an `opsw_lifecycle` of **Available**. Launch the NGUI and browse to **Unprovisioned Servers**. The list will be empty.

Perform a **Reload Cache** while on the **Unprovisioned Servers** view. The 50 servers will then be listed. Browse away and return to the **Unprovisioned Servers** view, the servers will not be listed.

Delete one of the 50 servers. Update the cache and browse away, return. The 49 servers will be listed. Add the server back to the pool, update the cache, browse away, and return and the servers are not listed again. Adding a 51st server causes similar behavior.

Resolution: Fixed

Bug ID: 160917

Description: Uncaught exceptions in `cogscript_ng`.

Platform: Independent

Subsystem: Command Engine

Symptom: There are uncaught exceptions in `cogscript_ng` that can cause a session to fail (the session dies and cannot run its commands on all the servers). These uncaught errors occur when there is an attempt to run commands on servers that no longer exist in the database.

Resolution: Fixed

Bug ID: 161205/161206

Description: pytz for tzdata2007k is available.

Platform: Independent

Subsystem: Command Engine

Symptom: Timezone packages have not been updated in a timely fashion.

Resolution: Fixed

Bug ID: 161169

Description: Editing large inherited custom attribute corrupts the name of the custom attribute.

Platform: Independent

Subsystem: Command Engine: Web Administration

Symptom: Create a large custom attribute (such as a certificate) for a facility, then go to one of the servers in that facility and try to edit the custom attribute. The name of the custom attribute will be corrupted after the edit.

Resolution: Fixed

Bug ID: 162844

Description: Australia timezone - DST occurs in old DST date (March 30 2008) in NGUI.

Platform: Independent

Subsystem: Opsware Command Engine Client Framework

Symptom: DST switchover is set for March 30 2008 (Old DST date) in the NGUI. The correct DST switchover date for Australian DST occurs April 6, 2008.

Resolution: Fixed

Bug ID: 163453

Description: Vista client must login twice to get into OCC.

Platform: Windows Vista

Subsystem: Data Access Engine

Symptom: When a Vista user logs in to the OCC, the new OCC login dialogue is displayed. After the user enters the userid/password and presses Enter, the older version OCC login dialog is displayed and the user must log in again.

Resolution: Fixed

Command-Line Interface

Bug ID: 165230

Description: OCLI: OverflowError : Description: long int too long to convert.

Platform: Windows NT

Subsystem: OCLI

Symptom: when running the `odownload` and `oupload` commands, `odownload` fails with an error, `oupload` uploads the package but also gives the following error:

```
File ".\controllers\word_upload_controller.py", line 12 1,
in _handle
OverflowError: long int too long to convert
Unknown Error Encountered
```

Resolution: Won't Fix

Communication Test

Bug ID: 161599

Description: Memory leak in `check_reachability`.

Platform: Independent

Subsystem: Communication Test

Symptom: The `check_reachability way-script` has a memory leak. When a `check_reachability` session terminates due to an unhandled exception, it leaks memory in proportion to the number of devices it processes. This causes the Command Engine (Way) to run out of memory. The leaked memory cannot be recovered without a Command Engine (Way) restart.

Resolution: Fixed

Data Access Engine

Bug ID: 157892

Description: Race condition in shadowbot connection handler.

Platform: Independent

Subsystem: Data Access Engine

Symptom: The Data Access Engine (spin) hangs and no longer fields requests.

Resolution: Fixed

Bug ID: 161876

Description: Agent installation fails on secondary Data Access Engine (spin).

Platform: Independent

Subsystem: Data Access Engine

Symptom: Agent installation fails with an unexpected error when the Agent resolves to a secondary Data Access Engine.

Resolution: Fixed

Bug ID: 162947

Description: `opswgw` install fails when Core Gateway is configured for spin load balancing.

Platform: Independent

Subsystem: Data Access Engine

Symptom: When spin load balancing is configured and none of the spins in the pool are primary, none of these spins are running a certgenerator. During a gateway installation, an is made to access a certgenerator locally instead of proxying to the primary spin causing an installation failure.

Resolution: Fixed

DCML Export Tool (DET)

Bug ID: 138466

Description: Export and import of a relocatable ZIP (with multiple instances in the source core) work correctly, but the summary statement of DET is incorrect

Platform: Independent

Subsystem: DET

Summary: If the user exports using a filter with `packageType = Relocatable_ZIP` that specifies multiple ZIP instances, the operation works correctly, exporting the ZIP instances as appropriate. A subsequent import also works correctly. However, the summary statement generated by DET during the export and import implies that just one ZIP instance was exported and imported even if multiple ZIP instances were involved.

Resolution: Fixed

Bug ID: 157557

Description: CBT baseline import crash.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: DET (CBT) fails to import after successfully completing a baseline export.

Resolution: Fixed

Bug ID: 161147

Description: Import of filter fails when there is an entry for **Custom Fields Schema Filter**.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: If you have a filter file with a **Custom Fields Schema Filter** entry in the `*.rdf` file, import of the RDF files fails with the error `Syntax error at line 11: invalid start tag`.

Resolution: Fixed

Bug ID: 161818/161914

Description: Software-migrated Solaris package instances cause `NullPointerExceptions` when imported as part of a software policy.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: After a software migration, it is possible for a `SOL_PKG` unit to be located in a folder and be associated with the customer *Software Repository* while the related `SOL_PKGINST` unit is still specified as *Customer Independent*. This causes the units to be located different places in the Software Repository. When the units are exported and imported into a different core, the DCML Export Tool cannot find SOL_PKGINST because it is generated in the directory of the parent rather than the `packages/any/` path.

This results in a fatal `NullPointerException` when a software policy containing one of these instances is also in the import (the DCML Export Tool expects to find this unit by `importedId` but can't).

Resolution: Fixed

Bug ID: 163067

Description: Units incorrectly assigned to folders in an export can not be added to a software policy.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: After a software migration, it is possible for a `SOL_PKG` unit to be in a folder and have customer *Software Repository* while the related `SOL_PKGINST` unit is still *Customer Independent*. This causes them to sit in different places in the Software Repository (word). If the units are then exported and imported into a different core, the CBT cannot find the `SOL_PKGINST` because it will be generated in the directory of the parent rather than the `packages/any/` path as it was on the Source Core.

This can then result in a fatal NPE if a software policy containing one of these instances is also in the import (the CBT expects to be able to find this unit by `importedId` but can't).

Resolution: Fixed

DSE

Bug ID: 161596

Description: Memory leak in `cogscript_ng way-script`.

Platform: Independent

Subsystem: DSE Backend

Symptom: The `cogscript_ng way-script` has a memory leak. Every `cogscript_ng` session leaks memory in proportion to the number of devices it processes. This causes the Command Engine (Way) to run out of memory. The leaked memory cannot be recovered without a Command Engine (Way) restart.

Resolution: Fixed

Gateways

Bug ID: 162916

Description: Default `ConnectionLimit` exceeds default `ulimit` on Solaris.

Platform: Independent

Subsystem: Gateways

Symptom: The default `ulimit` on Solaris is 256, while the default value for the Gateway `ConnectionLimit` is 1024. Therefore, in its default configuration, the Gateway could run out of file descriptors.

Resolution: Fixed

Bug ID: 163699

Description: Uninitialized memory on Solaris Gateway causes LB to malfunction.

Platform: Independent

Subsystem: Gateways

Symptom: An uninitialized memory bug causes the LB to malfunction on Solaris when the ingress and egress gateways are the same.

Resolution: Fixed

Bug ID: 164384/155031

Description: `portMap` update race condition detected.

Platform: Independent

Subsystem: Gateways

Symptom: The following error appears in LOF files:

```
2007-08-27T23:19:37,878Z ERROR 3 - ogthreads.c:2781
preconnector_thread: portMap update race detected... this should
not happen.
```

Resolution: Fixed

Global Filesystem (OGFS)

Bug ID: 137875

Description: Two different occurrences of `NameError` in `agentproxy.err`.

Subsystem: SAS Client - Global Shell/Shell Backend

Platform: Independent

Symptom: While running a registry snapshot operation from the Global Shell, the operation stalls, and error messages are written repeatedly to the `agentproxy.err` log file.

Resolution: Fixed

Bug ID: 150942

Description: Remote desktop sessions get disconnected, causing Windows patching to fail.

Subsystem: SAS Client - Global Shell/Shell UI

Platform: Windows

Symptom: Windows patching can fails when there is an active Remote Desktop session to the same managed server.

Resolution: Fixed

Bug ID: 159334/159502

Description: `SIGHUP / SIGPIPE` are set to ignore in remote terminal sessions/OGSH sessions not closing if they timeout causing orphaned processes.

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: When running remote terminals through OGFS, the signal dispositions are set differently than those from a raw SSH terminal; specifically `SIGHUP` and `SIGPIPE` are set to `ignore`. This can cause processes to be orphaned after a user has closed the remote terminal, especially when the user closes the terminal windows by using the windows' close button rather than by using the `Exit` or `Logout` commands. Processes can also be orphaned when a remote terminal session times out.

Resolution: Fixed

Bug ID: 164527

Description: `m2crypto` uses old-school python file (`stdio`) objects.

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: You see a `Too many open files` error in the `agentproxy.err` file. This condition could result in the stream logs having a zero byte size.

Resolution: Fixed

Localization

Bug ID: 158129

Description: DST problem for `BRT - America/Sao_Paulo`.

Platform: Independent

Subsystem: Localization

Symptom: SAS does not adjust to `BRT - America/Sao_Paulo` DST change in October 13th, 2007. For example, change the user's time settings in the SAS Client to `BRT - America/Sao_Paulo`. The result is the user's time in the SAS Client is one hour behind actual time.

Resolution: Fixed

OS Provisioning

Bug ID: 152551

Description: Ability to send notification at the end of a sequence/remediation job.

Platform: Independent

Subsystem: OS Provisioning Backend

Symptom: Email notification is sent at the end of the OS Sequence but before the remediation is finished. It's possible to send notification at the end of a remediation job, but not to send notification at the end of a *sequence/remediation* job.

Email notification should be sent after all underlying tasks have been complete (including remediation).

Resolution: Fixed

Bug ID: 163527

Description: Cannot run OS sequence with exception `stub rethrowing error after java.rmi.ServerException`.

Platform: Independent

Subsystem: OS Provisioning

Symptom: Java errors occur when trying to run OS Sequences

Resolution: Fixed

Bug ID: 163821

Description: OCC Client closes unexpectedly when creating a new OS Installation Profile.

Platform: Independent

Subsystem: OS Provisioning - OCC Client

Symptom: While creating a new OS Installation profile, the OCC Client closes with the error:

```
javaw.exe has encountered a problem and needs to close.  We are
sorry for the inconvenience.
```

Resolution: Fixed

Patch Management

Bug ID: 139208

Description: Using Patch Remediation to install ML01 on AIX 5.3 server produces errors.

Platform: IBM AIX 5.3.

Subsystem: Patch Management - Unix

Symptom: In some cases, using the Patch Remediation feature to install ML01 on AIX 5.3, the job will complete but with errors.

Resolution: Fixed

Bug ID: 157409

Description: Patch uninstallation job for APAR is completed but uninstall of APAR is pending.

Subsystem: Patch Management: Unix - Backend

Platform: Unix

Symptom: An attempt to remove AIX 5.3 APAR has a completed job status; however Uninstallation and Registration is in PENDING state.

Resolution: Fixed

Bug ID: 161495

Description: `java.lang.NullPointerException`: No patches imported when one of multiple selected patches does not have a specified URL.

Subsystem: Patch Management

Platform: Independent

Symptom: Certain Microsoft patches cannot be downloaded from their website, but instead must be obtained directly from Microsoft support, therefore the patch will not have a download URL. When you try to import these patches using the OCC, the import will fail.

Resolution: Fixed

Bug ID: 162442

Description: Web Services Data Access Engine (Twist) exception when viewing all patch policy exceptions on a Windows patch.

Subsystem: Patch Management: Windows - Backend

Platform: Windows

Symptom: The following error dialog is displayed when the user tries to view all patch policy exceptions on Windows 2003 Service Pack 2:

```
Received unexpected error, possibly due to network error. Please
check if your changes have already taken effect before retrying
this operation.
```

Resolution: Fixed

Bug ID: 163122

Description: Microsoft Office patch without metadata shows up as recommended on x86_64 platform.

Subsystem: Patch Management: Windows UI

Platform: Windows

Symptom: Certain Microsoft patches are displayed as **Recommended** on the x86_64 platform, even though there is no metadata for the patches.

Resolution: Fixed

Bug ID: 164738

Description: Packages imported using the OCC will fail if the import takes longer then 20 minutes.

Subsystem: Patch Management: Windows - Backend

Platform: Windows

Symptom: **Import from Vendor** fails after reaching the 20 minute upload limitation when importing a service pack or patches.

Resolution: HTTP/HTTPS requests adjusted to timeout after 60 minutes. If you need to increase/decrease the timeout interval, perform the following tasks:

1. Log in to the core server that hosts the OCC Web.
2. Edit the file `/etc/opt/opsware/httpsProxy/httpd.conf`.
3. Search for the entry: `Timeout 3600` (approximately line 12).
4. Change the value `3600` to the desired value. This value is the number of seconds until timeout, therefore if you want the request timeout to be an hour and a half, you would change the value to `5400` (90m x 60 = 5400s).
5. Restart the web server using the command:

   ```
   /etc/init.d/opsware-sas restart httpsProxy
   ```

Bug ID: 165016

Description: Remediation completed with error after installing SP2 on Windows 2003 x86.

Platform: IBM AIX 5.3.

Subsystem: Patch Management: Windows- Backend

Symptom: Doing an install of Windows Server 2003 SP2 with Agent 67, resulted in a failure that the Agent in the following error:

```
The request to retrieve information from the Opsware Agent
failed because it timed out.  If the problem persists, please
contact your Opsware Administrator.
```

Resolution: Fixed

Reconcile

Bug ID: 163334/150644

Description: `doer.py` modifies command results before they are written to the Data Access Engine (spin).

Subsystem: Reconcile Backend

Platform: Independent

Symptom: The Command Engine hangs during an HP-UX policy remediation that includes many packages.

Resolution: Fixed

Software Management

Bug ID: 159924

Description: Copy of existing software policy loses RPM settings.

Platform: Independent

Subsystem: Software Management API - Software Policy

Symptom: After copying an existing policy all of the new policy's RPM settings for the **Update Only**, **Version** and `Release` are set to the default values. The copy is not an identical copy. This also prevents users from easily creating a snapshot copy of an existing policy.

Resolution: Wont Fix - This behavior is fixed in release 7.0 and later.

Bug ID: 160824

Description: Packages unexpectedly removed during Software Policy remediation.

Platform: Independent

Subsystem: Software Management API – Software Policy

Symptom: When remediating a Software Policy that is almost identical to a previous policy except for a single package to be upgraded, packages that should not have been affected are removed.

Resolution: Fixed

Bug ID: 161339

Description: Yum multi-arch upgrade issue on x86_64.

Platform: Independent

Subsystem: Software Management: Backend - Remediate (RPM Packages)

Symptom: When attempting to install or upgrade a package that has a dependency on an x86_64 package, and the x86_64 package must also be upgraded to satisfy the dependency, Yum does not upgrade the x86_64 package.

Resolution: Fixed

Bug ID: 161577

Description: Interleaving can cause RPM upgrades to fail if installed RPMs require the same versions of other installed RPMs.

Platform: Independent

Subsystem: Software Management: Backend - Remediate (RPM Packages)

Symptom: When installed RPMs have strict version requirements, pre-existing dependencies can cause package upgrades in software policies to fail if the upgrade affects a package on which another package has a dependency.

Resolution: Fixed

Bug ID: 161849

Description: 6.5 job status missing information for application configuration remediation.

Platform: Independent

Subsystem: Software Management UI - Install/Uninstall/Remediate

Symptom: **Configure Application** provides no additional data in 6.5.x. In 6.0.x the column **Item** exists but this column does not exist in 6.5.x. Therefore, it's not possible for the end user to know which application configuration failed in 6.5 without checking the way log files.

Resolution: Fixed

Bug ID: 162282

Description: Solaris packages with the same name have naming conflicts with response files.

Platform: Independent

Subsystem: Software management Tools - Other

Symptom: This problem occurs because of the way the Software Repository identifies packages. Packages are identified by name and location, not on the Unit ID. Therefore, when a new file with the same name as an existing file is uploaded, the Software Repository finds and updates the old one instead of creating a new one.

Resolution: Fixed

Bug ID: 162475

Description: Remediate has implicit one hour timeout for unit scripts

Platform: Independent

Subsystem: Software Management: Backend - Remediate (Other)

Symptom: Certain devices such as ZIP drives timeout during remediation. The `SCRIPT_TO` in the `action_blob` is now configurable via the system configuration, with a default value of one hour (up from 20 minutes) with the key of `way.remediate.script_alarm_timeout`.

The `maxruntime` attribute is set to the time left in the session with a minimum of one hour if there is less time than that remaining.

Resolution: Fixed

Bug ID: 163070

Description: SW Policy changes require removal of vital components.

Platform: Independent

Subsystem: Software Management API - Software Policy

Symptom: You have a Software Policy that contains core packages and patches which can not be detached. You must be able to detach and update the packages and patches together and then remediate the server.

Resolution: Fixed

Bug ID: 163071

Description: The same packages exist in both the install and remove lists.

Platform: Independent

Subsystem: Software Management: Backend - Remediate (RPM Packages)

Symptom: The same packages existing in both the install and remove lists caused confusion.

Resolution: Fixed

Bug ID: 163134

Description: Only one of what should be three **removed-as-side-effect**s were shown in the UI.

Platform: Independent

Subsystem: Software Management: Backend - Remediate (RPM Packages)

Symptom: After a package upgrade, the Jobs and Sessions view displayed only two units as **removed-as-side-effect** when three were actually removed.

Resolution: Fixed

Bug ID: 163274

Description: **Installed-as-side-effect** units are intermixed with the units that were actually installed.

Platform: Independent

Subsystem: Software Management: Backend - Remediate (Other)

Symptom: The NGUI **Jobs and Sessions** view has formatting and sorting errors.

Resolution: Fixed

Bug ID: 163328

Description: `Error 21: The device is not ready` not handled by `NtPlatform::reboot()`.

Platform: Windows

Subsystem: Software Management: Backend - Remediate (Other)

Symptom: A call to the WIN32 API function `InitiateSystemShutdown()` fails with the error code `ERROR_NOT_READ(21) - "The device is not ready"` preventing a reboot.

Resolution: Fixed

Bug ID: 163377

Description: Duplicating packages and uninstalls.

Platform: Independent

Subsystem: Software Management: Backend - Remediate (Other)

Symptom: When the same RPM is duplicated in the library but with different IDs, remediate treats the packages as unique and not as duplicate instances of the same package causing unexpected results.

Resolution: Fixed

Bug ID: 163417

Description: Installing APARs should better emulate `instfix` by including requisites.

Platform: AIX

Subsystem: Software Management API – Reconcile

Symptom: When you install an APAR, only those filesets directly referenced by the APAR are installed, dependencies are not. Also, if an APAR fileset is missing dependencies, it is dropped it with the error `Cannot install, missing dependencies`.

Like `instfix` remediate should check to see if the dependent filesets are available in the Software Repository and, if so, add them with a message that they're being installed to satisfy dependencies.

Resolution: Fixed

Bug ID: 163452

Description: OCC doesn't update the status of deleted packages even though they were already deleted from the Software Repository.

Platform: Independent

Subsystem: Software Management – OCC

Symptom: When you delete a software package using the SAS Client, the package is deleted from the Software Repository but still appears in the SAS Client's list of software packages.

Resolution: Unable to Reproduce

Bug ID: 164107

Description: Duplicating packages and uninstalls.

Platform: Independent

Subsystem: Software Management: Backend – Remediate

Symptom: You have an RPM that appears twice in the Library, for example:

- `/System Utilities/Red Hat Enterprise Linux AS 3/ ismruntime-rpm-3.3.9-1.i386` (**ID 22840001**)
- `/System Utilities/ismruntime-rpm-3.3.9-1.i386` (**ID 22710001**)

You have two policies that reference these RPMs:

- P1 includes 22840001
- P2 includes 22710001

You attach and remediate P1 and P2 onto the same server. As expected, `ismruntime-rpm-3.3.9-1.i386` is installed only once.

However, if you then detach and remediate P2 from that server, `ismruntime-rpm-3.3.9-1.i386` is removed which is unexpected as it should not be removed.

Resolution: Fixed

Bug ID: 164323

Description: App compliance may not be correct after remediating Solaris patches.

Platform: Solaris

Subsystem: Software Management – Remediate (Other)

Symptom: When doing Solaris patching, some of the selected patches may not be installable on a particular device (for example, hardware incompatibilities, the software it patches isn't installed, and so on). Therefore, when remediation tries to install one of these patches, it fails with an exit code that is interpreted by Remediate as benign and so no errors are issued. When application compliance runs, there is no record of the patches not being installable on that device, so application compliance marks the device as out of compliance.

Resolution: Fixed

Bug ID: 164812

Description: Remediate scripts still have memory leaks.

Platform: Independent

Subsystem: Software Management Backend– Remediate (Other)

Symptom: Unable to reproduce any case that causes a memory leak with current scripts.

There are objects, even large numbers of objects, but when the system is allowed to quiesce, the objects are all properly garbage collected.

Resolution: Unable to Reproduce

Bug ID: 165042

Description: Mixed Mesh - Software compliance displays *Not Applicable* after attaching server to policy.

Platform: Independent

Subsystem: Software Management API– Compliance

Symptom: In a mixed mesh environment, Software compliance displays *Not Applicable* after attaching server to policy. Software Compliance status is updated only after running remediation. This is intended behavior.

Resolution: Wont Fix

Virtualization

Bug ID: 162448

Description: `nfs4_domain` setting regarding the zone create in Solaris.

Platform: Sun Solaris

Subsystem: Virtualization - Backend (Zones)

Symptom: Zone creation/booting on U4 asks for user input (with the message: `Confirm the following information. If it is correct, press F2`) because the `nfs4_domain` setting is not added to the `sysidcfg` file.

Resolution: Fixed

Visual Analyzer

Bug ID: 164707

Description: Sitemap fails to gather the process list on Windows 2003.

Platform: Windows Server 2003

Subsystem: Visual Analyzer: Sitemap

Symptom: Sitemap fails to gather the process list on certain Windows Server 2003 servers due to a permission configuration on those servers that prevents gathering the process list.

Resolution: Fixed

Visual Packager

Bug ID: 164841/164515

Description: Mixed Mesh-Remediate audit custom script fails when run from slave core on server in master core with 6.61 Agent.

Platform: Independent

Subsystem: Visual Packager: Backend

Symptom: You create an Audit with a custom script and target Windows server in a master core with a SAS 6.61 Agent. Run this Audit from a Slave core. Now, run the Remediate Audit script from the Slave core. The Remediate audit script fails with error.

Resolution: By Design – SAS 6.61 Agents require that the core be SAS 6.61.

Bug ID: 165314

Description: Visual Packager does not create the policy and the package.

Platform: Independent

Subsystem: Visual Packager: Backend

Symptom: Select Actions ➤ Create Package. The job runs successfully with no errors but the package is not created in the **Packages** channel and the Software Policy is not created in the specified location.

Resolution: Wont Fix

Web Services Data Access Engine

Bug ID: 160441

Description: `DataAccess-session.jar` should have timeouts increased.

Platform: Independent

Subsystem: Web Services Data Access Engine

Symptom: The timeout settings in `DataAccess-session.jar` are set too low by default causing Web Services Data Access Engine timeouts.

Resolution: Fixed

Bug ID: 162182

Description: Problem with nested software policies.

Platform: Independent

Subsystem: Web Services Data Access Engine

Symptom: if you attach a Software Policy that contains another Software Policy (nested Software Policies) to a server, the custom attributes configured in the child Software Policy are not attached to the server.

Resolution: Fixed

Chapter 5: Known Problems, Restrictions, and Workarounds in Opsware SAS 6.61

IN THIS CHAPTER

This chapter describes workarounds for known problems in Opsware SAS 6.61. These descriptions are arranged by the following features:

- Agents
- Application Configuration
- Audit and Remediation
- DCML Exchange Tool (DET)
- Gateways
- Global Filesystem/Shell
- Health Check Monitor
- ISM Tool
- Jobs and Sessions
- Microsoft Windows PowerShell/SAS Integration
- NAS/SAS Integration
- Operating System Provisioning
- Patch Management for Windows
- Patch Management for Unix
- Remediation
- SAS Client
- SAS Client Reports
- SAS Installer

• SAS Web Client • Software Management • Virtualization • Visual Application Manager (VAM) • Visual Packager	

Agents

Bug ID: 129735

Description: Scanning a managed server opens the Unmanaged Server window.

Subsystem: SAS Client, Opsware Discovery and Agent Deployment (ODAD)

Platform: Independent

Symptom: When you scan a server that is already managed by Opsware SAS, the ODAD feature cannot determine which managed server ID it corresponds to and, by default, opens the Unmanaged Server window.

Workaround: None

Bug ID: 166283

Description: Agent Upgrade from custom extension fails.

Subsystem: Agent Deployment/Upgrade

Platform: Windows 2003

Symptom: When upgrading an Agent from a custom extension on a Windows 2003 machine, the Agent is upgraded, but with an error. The Agent is, in fact, upgraded but there is an error in notifying the Core that the Agent has been upgraded.

Workaround: None

Application Configuration

Bug ID: 137456

Description: Preserve format does not preserve comments when a comment exists on a line that has been deleted.

Platform: Independent

Subsystem: Application Configuration

Symptom: With preserve format enabled, any change to the value set that causes a line to be deleted from a configuration file will result in any comments on the deleted line to be removed also.

Workaround: None

Bug ID: 138610

Description: Device Group Explorer not displaying inherited values correctly for servers which belong to multiple groups with identically named application configurations.

Platform: Independent

Subsystem: Application Configuration - Device Groups

Symptom: If two different device groups contain an application configuration that uses the same name, and each group has different values set for the configuration, and the same server belongs to both groups, then the Device Group Explorer will not show the proper inherited values when that server is displayed. It will only show the inherited values of the current device group in the browser and not both groups.

However, when you view the application configuration in the server's Device Explorer, you will see the value inheritance correctly.

Workaround: In general, if you want the application configuration instance of a server to be separate from the device group that the server belongs to, use a different name for each application configuration instance.

Bug ID: 139042

Description: Audit and Remediation - Application Configuration Rule View rule changes are not updated right away following rule modifications.

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rule

Symptom: If you add or make changes to remediation application configuration rule (audit, snapshot, audit policy) in the Rule View tab, such as changing a value in Operator, Reference, and the Value drop-down lists, you will not see the changes reflected in the rule text, even though the changes will be made.

Workaround: To see the changes in the Rule View tab:

1. Save the changes.
2. Select the File View tab.
3. Select the Rule View tab

Bug ID: 161122/161124

Description: NGUI freezes when removing an appconfig from a server group with 50 servers.

Platform: Independent

Subsystem: Application Configuration

Symptom: When removing an appconfig instance in the server browser for a server group with 50 or more servers, the NGUI appears to freeze. If enough time passes, the NGUI will become responsive again, however, if you then select **Save Changes**, the NGUI will time out and freeze (BZ #161124).

Workaround: None

Bug ID: 166365

Description: Conflicts occur when running remediate policy containing appconfig.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: Multimaster conflicts can result when scanning compliance for Software and Application Configuration in succession via the *Dashboard*.

This can happen under the following scenario:

1. A user is logged in to the OCC Client in core A.

2. The User is looking at the compliance dashbaord for a server that is in core B.
3. The server has an attached policy that also contains application configurations.

If the user clicks the **Scan Now** buttons for Software and Application Configuration in immediate succession, multimaster conflicts will result.

Workaround: Do not click the **Scan Now** buttons in succession within a short period of time. Click **Scan Now** and wait for a reasonable amount of time before clicking another **Scan Now** button, if necessary.

If multimaster conflicts have already occurred, they must be resolved by a user that has permissions to the Multimaster Tools console in OCC Web.

Bug ID: 166540

Description: Conflicts occur when running remediate policy containing appconfig.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: Software compliance can indefinitely remain in the scanning state.

This can happen under the following scenario:

1. A user is logged in to the OCC Client in core A (assuming a Multimaster Mesh).
2. The user is looking at the compliance dashbaord for a server that is in core A.
3. The server has an attached policy that also contains application configurations.

If the user clicks on the **Scan Now** buttons for Software and Application Configuration in succession, the Software compliance could remain in the scanning state.

Workaround: Do not click the **Scan Now** buttons in succession within a short period of time. Click **Scan Now** and wait for a reasonable amount of time before clicking another **Scan Now** button, if necessary. You can click **Scan Now** again for Software compliance (applies only to Software compliance) and it will correctly update the status.

Audit and Remediation

Bug ID: 137898

Description: Some Audit and Remediation CIS Rules/Checks will not run in an Audit if the proper file is uploaded to the core.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: Some Audit and Remediation CIS Rules/Checks in an Audit require that the files auditpol.exe, ntrights.exe, and showpriv.exe exist on the core that the Audit is running from. If this file does not exist on the core, then when a user runs an Audit with specific CIS Rules/Checks that require this file, then the user will see a time out in the Audit job.

Workaround:

1. Get the Windows utilities (`showpriv.exe, ntrights.exe, auditpol.exe`) from the Microsoft Windows 2000 Resource Kit.
2. Install the OCLI on a UNIX server managed by Opsware, or on an Opsware core server.
3. Copy the Windows utilities to `/var/tmp` on the UNIX server.
4. Make sure `/opt/opsware/agent/bin` is at the beginning of the PATH

   e.g. `export PATH=/opt/opsware/agent/bin:$PATH`
5. Run the following three OCLI commands:

```
oupload  -C"Customer Independent"  -t"Windows Utility"  -
O"Windows 2003"  --old  /var/tmp/showpriv.exe

oupload  -C"Customer Independent"  -t"Windows Utility"  -
O"Windows 2003"  --old  /var/tmp/ntrights.exe

oupload  -C"Customer Independent"  -t"Windows Utility"  -
O"Windows 2003"  --old  /var/tmp/auditpol.exe
```

6. Perform the following steps to validate the file upload:

   a) Using the SAS Client, go to **Opsware Administration**.

   b) Go to **Patch Settings**

   c) Look at the list of **Patch Utilities** to determine that each of the three utilities are listed and on the core. If any one of the files is not listed, then they must be uploaded/imported into the core.

Bug ID: 137901

Description: Application Configuration Audit Rules syntax limitation for "does not contain" rule

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rules

Symptom: The Application Configuration Rules for Audit and Remediation (audits, snapshots, and audit policies) has a limitation in that you should not create a rule that uses the syntax *Does Not Contain* twice in the same rule.

Workaround: Avoid using *Does Not Contain* more than once in an application configuration Audit and Remediation rules.

DCML Exchange Tool (DET)

Bug ID: 138949

Description: Some imports fail if Microsoft patches are missing.

Platform: Windows

Subsystem: DET

Summary: By design, DET doesn't allow the import of Microsoft patches; they must be inserted into Opsware by the MS patch database import process. Thus, if an export contains a Microsoft patch and the destination mesh is not up-to-date with regard to MS patches, the import will not import the missing patches. It will print a warning at the end like this:

```
The following Windows patches were not uploaded:
Q911564 (WindowsMedia-KB911564-x86-ENU.exe)
```

The behavior described in the preceding paragraph is not a bug. However, associated objects in the failed import will not be imported as a side effect. For example, if you import a folder or a device group with multiple attachments (such as software policies or OS sequences) and the import also contains a Windows patch that does not exist in the destination mesh, then the import fails and the attached objects are not imported.

Workaround: Import MS patches with the SAS Client feature that relies on the MS patch database. Then, you can import the other objects (such as software policies) with DET.

Bug ID: 135494

Description: Import correctly detaches and deletes objects, but preview incorrectly states that the objects will be renamed.

Platform: Independent

Subsystem: DET

Summary:

1. Create a template with two applications in it. Export this from mesh A and import into mesh B.
2. Detach one application from the template and incrementally export with `-del`. This export will contain the detachment and the delete of the application.
3. Preview the import with `-del`, then perform the import with `-del`.

In this scenario, the preview incorrectly shows that the application will be renamed because it is in use by a template. The actual import will correctly delete the application. This problem also occurs when other objects are detached and deleted, for example, application/package, application policy/application policy, and so forth.

Note that this problem does not occur if *both* objects are being deleted, only if one object is being deleted and detached from the other.

Workaround: None

Gateways

Bug ID: 146262

Description: The `/var/log/opsware/opswgw-lb` directory is not created by the installer.

Platform: Independent

Subsystem: Opsware Installer

Symptom: The `/var/log/opsware/opswgw-lb` directory is not created by the installer, therefore, the load balancer gateway starts without a problem, but there is no logging directory and, therefore, no logs.

Workaround: Manually create the `/var/log/opsware/opswgw-lb` directory.

Bug ID: 147215

Description: Uninstallation of a Core Gateway does not remove certificates.

Subsystem: Opsware Gateway

Platform: Independent

Symptom: When the Core Gateway is uninstalled, the Opsware Installer does not remove the data under `/var/opt/Opsware/crypto/opswgw-cgw0-<DCNAME>`. This can cause a problem if the core is reinstalled with a different crypto database because the certificates will no longer be valid.

Workaround: Remove old Gateway crytpo files.

Bug ID: 149334

Description: Running the Opsware Installer with the `-a` option does not accept uploads if it is in the same action file as other components.

Subsystem: Opsware Installer

Platform: Independent

Symptom: You tried to install a core using an action file similar to the following:

```
[root@ruby1 root]# cat action_file1
%components
truth
owc
word
spin
way
osprov_buildscripts
osprov_boot
osprov_media
gateway_ha
shell
word_uploads
osprov_stage2s
oracle_sas
```

In this case, since the Opsware Installer is run from the primary distro, the content upload fails. The Opsware Installer prompts you for the upload distro, but does not accept the valid entry.

Workaround: Remove the `word_uploads` and `osprov_stage2s` entries from the primary action file and create a new action file to be used by the Opsware Installer when it is run from the upload distro.

Bug ID: 151558

Description: A fresh install of the Spin fails due to missing baseline/seed data.

Subsystem: Opsware Installer

Platform: Red Hat Linux 4AS x64

Symptom: During the Model Repository installation phase during a fresh installation, the Opsware Installer does not completely insert the baseline data. Specifically, Oracle may not insert certain baseline data into the `role_classes` table as well as other tables. This is an intermittent and a silent error because Oracle generates no errors, failures, or trace files. The Opsware Installer appears to complete the Model Repository installation successfully, however, the subsequent installation of the Model Repository Multimaster Component fails due to the missing baseline data.

Workaround: Before beginning the installation/upgrade:

1. Shutdown all SAS components, if necessary.
2. On the server hosting the Model Repository run these commands:

```
Su - oracle
Sqlplus "/ as sysdba"
ALTER SYSTEM SET EVENT='12099 trace name context forever,
level 1' SCOPE=SPFILE;
Shutdown immediate;
Startup
Exit
```

3. Start the Opsware Installer and install/upgrade the Model Repository.

Global Filesystem/Shell

Bug ID: 129237

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

Subsystem: SAS Client - Remote Terminal, Global Shell

Platform: Independent

Symptom: In the SAS 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 SAS Client and then open a new terminal window for a Windows or Unix server.

Bug ID: 130514

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

Subsystem: SAS 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: 137948

Description: File system is accessible under `/opsw/Application/` after removing the application node from the server.

Subsystem: SAS Client - Global Shell

Platform: Independent

Symptom: You created an application node under Application Servers from the SAS Web Client and then assigned it to a server. Using the SAS Web Client, you removed the node from the server. From Global Shell, you could still access the file system under the `/opsw/Application` model space that showed the node.

Workaround: Launch a new Global Shell session to access the file system of a server under `/opsw/Application` that shows the node was removed.

Bug ID: 139095

Description: Default Global Shell prompt (PS1) overwrites single-line output.

Platform: Independent

Subsystem: Global Shell

Summary: The default PS1 that ships with Opsware SAS includes a carriage return (`\r`), which seems to overwrite output that does not contain a newline. This problem occurs often with the OCLI methods, since attribute files and method results do not typically contain newlines. It also affects the viewing of custom attribute values.

Workaround: Edit`.bash_profile`, change the PS1 setting to the following:

```
PS1="[\uOGSH \W](\!) $"
```

Bug ID: 133316

Description: On Solaris OGFS, `rosh` (`ttlg`) commands for Windows file systems are case sensitive.

Platform: Solaris (OGFS), Windows (managed server)

Subsystem: Global Shell

Summary: This problem occurs only if the OGFS (hub) is running on Solaris, not on Linux. It occurs when a user in a Global Shell session `cd`'s into a Windows file system directory and issues a `rosh` (`ttlg`) command that uses a different case than what appears in the OGFS. Although the names in a Windows file system are not case sensitive, the hub is hosted on a Unix server and is restricted by Unix file system semantics for case sensitivity.

For example:

```
$ pwd
/opsw/Server/@/m229/files/Administrator/
$ cd c
$ ttlg -l Administrator dir c:\\
ttlg: Error getting current directory (1161): No such file or
directory
$ cd ../C
$ ttlg -l Administrator dir c:\\
 Volume in drive C has no label.
 Volume Serial Number is 6836-A79C
```

Workaround: You must observe Unix filesystem case semantics even when you have changed into a Windows server's file system. The Global Shell's tab completion feature automatically accounts for case sensitivity.

Bug ID: 137948

Description: Under OGFS, the file system under `/opsw/Application/` is still accessible even after an application node is detached from a server.

Platform: Independent

Subsystem: OGFS

Summary: Scenario: you create an application node under **Application Servers** in the SAS Web Client and attach the node to a managed server. In the Opsware Global Shell, you `cd` to the server's file system under the node, as in the following example:

```
cd /opsw/Application/Application Servers/<app-server>/@
cd Server/<server>/files/root
```

In the SAS Web Client, you detach the application node from the server, however, in the Global Shell you can still access the server's file system under the detached node.

Workaround: Exit the current Global Shell session and start a new one.

Bug ID: 140328/158788

Description: The OGFS cannot handle files larger than 2 GB.

Platform: Independent

Subsystem: Global File System - Backend

Symptom: In a Global Shell session, if you try to copy a file larger than 2 GB from a server's directory an error occurs, for example:

```
$ pwd
/opsw/Group/Public/bw-window-group/@/Server/m229/files/bw1/C
$ cp ddd
cp: reading `ddd': File too large
```

```
$ ls -l ddd
-rw-r--r-- 1 502 502 18446744072062238720 2007-03-31 06:48
ddd
```

Workaround: None

Bug ID: 140696

Description: In `rosh`, an interactive Windows program hangs.

Platform: Windows

Subsystem: Global Shell

Symptom: Launch a Global Shell session, `rosh` on a Windows managed server, run an interactive program such as `ismtool`. The interactive program will hang.

Workaround: None, unless you have access to the source code of the Windows interactive program. To fix the code, for example in Python, call the `sys.stdout.flush()`.

Bug ID: 143198/130717

Description: OGFS installation fails if the `hugemem` kernel is installed.

Platform: Linux

Subsystem: Global File System - backend

Symptom: TBD

Workaround: Before installing the OGFS, log on to the OGFS server as `root` and enter the following:

```
cd /usr/src/
ln -s linux-2.4.21-47.EL linux-2.4.21-47.ELhugemem
```

Run the Opsware Installer again to install the OGFS.

Bug ID: 144661

Description: The `rosh -n` and `-l` options should not be required when invoked from `/opsw/Server/@/<server>/metabase/<user>`.

Platform: Windows Managed Server

Subsystem: Global Shell

Symptom: The `rosh` command generates the following error message: `Username must be specified with -l or via path`. The error occurs when `rosh` is invoked without `-n` or `-l` from within the `<user>` subdirectory of metabase, registry, or complus. The error does not occur in under the files subdirectory.

Workaround: Specify the user name (Windows login) with the `-l` option.

Bug ID: 148571

Description: Cannot copy read-only files to a managed server using the OGFS.

Platform: Independent

Subsystem: Global File System - backend

Symptom: When using the OGFS to copy read-only files to the file system of a managed server as a non-root user, `cp` may return a `Permission Denied` error. The target file will be created, but it will be empty. Example:

```
$ pwd
/opsw/Server/@/server-1/files/non-root/tmp
$ echo abc > abc
$ chmod -w abc
$ ls -l abc
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
$ cp abc ABC
cp: cannot create regular file `ABC': Permission denied
$ ls -l abc ABC
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
-r--r--r-- 1 59820 1 0 2007-05-08 23:01 ABC
```

Workaround: If the `cp` command fails, make the target file writable, retry the `cp` command, and then make the file read-only (if necessary) after the copy is completed. Example:

```
$ ls -l abc ABC
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
-r--r--r-- 1 59820 1 0 2007-05-08 23:01 ABC
$ chmod +w ABC
$ cp abc ABC
$ ls -l abc ABC
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
-rw-r--r-- 1 59820 1 4 2007-05-08 23:01 ABC
$ chmod -w ABC
```

Bug ID: 149155/161446

Description: Installation of the Opsware SSH server might not correctly patch `/etc/nsswitch.conf`.

Platform: Independent

Subsystem: Global File System - Backend

Symptom: The `OPSWsshd` install process must patch the `passwd` entry of the `/etc/nsswitch.conf` file. It is unable to do so if the `passwd` entry is missing (as it is in some default Solaris configurations) or is commented out.

This problem has the following symptoms:

- The SAS Client fails to initialize properly and issues the message "`Spoke initialization failed. See Java console for details`".
- `ssh` (on port 2222) to the OGFS fails.
- `ssh` (on port 2222) to the OGFS results in a normal login shell if the user has a local account on the OGFS server.

Workaround: Before installing Opsware SAS, ensure that the `nsswitch.conf` file on each OGFS server contains a valid `passwd` entry. According to the Solaris manual `nsswitch.conf(4)`, the default value is:

```
passwd: files nis
```

(Note that this default value might not be a suitable value all sites.)

If you experience this problem after installing Opsware SAS, fix the `/etc/nsswitch.conf` file on each OGFS server as described above and run the following command as `root`:

```
/opt/opsware/bin/python \
/opt/opsware/sshd/libexec/editnsswitch.py \
--action add --db passwd --plugin opsware_ns \
--file /etc/nsswitch.conf
```

This workaround also prevents the issue described in Bug ID: 161446: Spoke initialization fails.

Health Check Monitor

Bug ID: 155229

Description: If you run certain global probes on a server with only the Model Repository installed you get the message `ImportError: No module named librpc.`

Subsystem: Health Check Monitor

Platform: Solaris

Symptom: The Health Check Monitor requires `librpc` to be installed. The *Opsware® SAS Administration Guide* instructs users to run global health checks on the server that hosts the Model Repository. The Opsware SAS installation does not install `librpc` on this server so the global health check fails.

Workaround: A global health check should be run from the server that hosts the Primary Core's Model Repository Multimaster Component (`spin`).

ISM Tool

Bug ID: 164241/130347

Description: Cannot run ismtool - build: Msi API Error.

Platform: Windows Server 2003

Subsystem: ISM Tool

Symptom: Attempting to run the command ismtool --build <filename. fails.

Workaround: Always `cd` to the working directory in which the ISM directory located. Do not use the full path when invoking the ISMtool.

Jobs and Sessions

Bug ID: 139762

Description: The NGUI and OCC web display different job IDs for the same jobs.

Subsystem: Jobs and Sessions

Platform: Independent

Symptom: You schedule the installation of a server patch to run later. The pending job is assigned different IDs in the NGUI and the OCC. The Oracle view, `TRUTH.JOBS,` is also affected.

For example, the NGUI may identify a pending job as `Job 13880001` while the OCC identifies the same job as `Job 13930001`.

Workaround: None

Bug ID: 160883

Description: Reopening the Jobs window before a scheduled job has run can cause the incorrect status for that job to be displayed.

Subsystem: Jobs and Sessions

Platform: Independent

Symptom: For example:

1. Scheduled a remediation job, then close the job.
2. Click on the job log to reopen the Jobs windows before the job's scheduled start time. The job status shown in this window is not updated.
3. Let the job start and finish.
4. Click on f5

The job list shows the job as completed. Double click to open the completed job. The old job status is still displayed. I appears that, if the user closes the Jobs window, the cache is not cleaned up for scheduled jobs.

Workaround: Close the job window using the "Close" option.

Microsoft Windows PowerShell/SAS Integration

Bug ID: 158487

Description: PowerShell MSI does not install successfully on Vista.

Subsystem: Microsoft Windows PowerShell/SAS Integration

Platform: Microsoft Vista

Symptom: Microsoft Windows PowerShell installations, using the MSI file on Windows Vista, fail with message code: `2869`. The is a Microsoft bug: by default, the Administrator account no longer has superuser privileges enabled.

Workaround: You can *Run As Administrator*, temporarily enabling superuser privileges, and the MSI file will successfully execute the PowerShell installation.

NAS/SAS Integration

Bug ID: 148482

Description: Duplex reporting does not work on all Opsware supported operating systems.

Subsystem: SAS Client - NAS Integration

Platform: Independent

Symptom: Opsware does not report duplex for Linux on hardware that does not support the `ethtool` command, such as Sun Fire V20z and Sun Fire X2100.

Workaround: None

Bug ID: 149148

Description: NAS and SAS are slow to reflect the correct configuration after a port change.

Subsystem: SAS Client - NAS Integration

Platform: Independent

Symptom: Consider this scenario: in a NAS/SAS integration, a managed server is connected to a switch. You unplug the network cable from the switch for this managed server. You then plug the cable back in to the switch, but to a different port on the same VLAN. Both SAS and NAS continue to display the original configuration, instead of the correct (current) configuration. This can cause `Unknown Configuration` and duplex mismatch errors on the Server Compliance Report.

Workaround: Run the NAS Topology Data Gathering diagnostic tool on the (single) switch to get the latest configuration data. See the *Opsware*® *SAS User's Guide: Server Automation* for more information about this diagnostic.

Operating System Provisioning

Bug ID: 133894/143395

Description: Wordbot error during import media.

Subsystem: OS Provisioning - import_media

Platform: Independent

Symptom: There appears to be a bug in the mechanism that connects to the Data Access Engine, retrieves customer information associated with the IP address of a request to the Software Repository server, and then caches it. Rarely, this results in a `wordbot.accessDenied` error.

Workaround: None. This error is caused by a rare transient problem within the Software Repository. The import_media script will retry each package upload three times, which is normally sufficient to work around this issue. If you see this message logged frequently and the affected package is not correctly uploaded even with the retries, contact Opsware Support.

Bug ID: 135253

Description: Cannot reprovision a recently provisioned server sooner than ten minutes after provisioning the server.

Platform: Linux, Solaris

Subsystem: OS Provisioning - Reprovisioning a Server

Symptom: If you provision a server and attempt to reprovision the same server within ten minutes, the reprovisioning will fail.

Workaround: Wait ten minutes before attempting to reprovision or reboot the server.

Bug ID: 138234

Description: Hardware registration information for servers listed in the SAS Web Client's Server Pool and the SAS Client's Unprovisioned Server list is spontaneously disappearing.

Platform: Windows XP

Subsystem: OS Provisioning

Symptom: In some cases, Windows XP servers that have been added to the Server Pool in the SAS Web Client or Unprovisioned Servers list in the SAS Client will initially report hardware registration information, but after a certain period of time, the server will stop reporting hardware information and all previously reported information will disappear.

Workaround: Reboot the server into the Server Pool.

Bug ID: 139689

Description: Creating a second OS Installation Profile from second instance of SAS Client launched from the SAS Web Client as a different user will cause SAS Client to crash.

Platform: Independent

Subsystem: OS Provisioning - OS Installation Profiles

Symptom: If you create an OS Installation Profile from inside the SAS Web Client, then launch the SAS Client from the SAS Web Client and log in as different user, and attempt to create another OS Installation Profile as the second user, the SAS Client will crash.

Workaround: None. This scenario is hopefully unusual and is not supported.

Bug ID: 143327

Description: PXE boot of Windows 2003 x86_64 VM using DOS native drivers build agent fails with "`DHCP servers not responding`".

Subsystem: OS Provisioning

Platform: Windows

Symptom: PXE booting a ESX 3.0.1 Windows 2003 x86_64 VM using the Windows build agent fails with the message "`DHCP servers not responding`", even though the DHCP server is up-and-running.

Workaround:

1) Use the "`undi`" PXE boot image.

or

2) Use the "`winpe64`" PXE boot image.

Bug ID: 143459

Description: Scenario: a server the customer assignment “Not Assigned”. Attempting to provision that server causes the server to be assigned to the default customer. When you attempt to reassign the server to “Not Assigned”, an error occurs.

Platform: Independent

Subsystem: OS Provisioning/Customer Assignment

Symptom: If you provisioned a sever that had a customer assignment set to “Not Assigned”, and then provision the server with an OS Profile or OS Sequence that has a customer the server will be assigned to the customer set in the OS Profile or OS Sequence. However, if you attempt to change the server's customer assignment back to “Not Assigned”, you get an error. Not Assigned is an invalid customer assignment post-provisioning

Workaround: None

Bug ID: 143503

Description: OS Provisioning Process Completes Successfully but Remediation not Always Succeeding.

Platform: Independent

Subsystem: OS Provisioning

Symptom: During OS provisioning certain access permissions to the servers and objects used in the OS Sequence are not checked at the beginning of the install OS job. These permissions are checked after the OS installation is complete and prior to the remediate job. Permissions problems, such as not having write access to the Customer assigned to the server by the OS Sequence, can cause this remediate job to fail silently.

Workaround: Make sure your user belongs to a group that has access to all servers and objects required by the specific OS Provisioning job.

Bug ID: 144615

Description: Unable to save the change of OS Sequence Remediation's Script Timeout using Save Changes dialog

Platform: Independent

Subsystem: OS Provisioning - OS Sequence with Remediation

Symptom: You create an OS Installation Profile, and in the Remediate Policies task object, enable remediation. In an Ad-Hoc Script you set a Script Timeout value. The timeout value will be saved when you close the OS Sequence and click **Yes** to save changes, or if you use the **File menu ➤ Save** function.

However, if after you save this initial configuration you open the OS Sequence again and make a change to the script timeout value, and then attempt to close the OS Sequence, you will be prompted to save the changes in a dialog. If you click **Yes,** the changes will not be saved.

Workaround: During OS Sequence modification phase, in order to save your changes to the Script Timeout field in an Remediate Policies object, click the mouse to empty boxes (such as Command box) to make the OS Sequence object window dirty. The changes would then be saved through either methods (through **File menu ➤ Save**, or close the OS Sequence Window and choose Yes to save).

Bug ID: 148335

Description: VMware guests with more than one network interface cannot connect in DOS boot image.

Platform: Independent

Subsystem: OS Provisioning/Network Booting

Symptom: If, when network booting a VMware guest machine via the DOS boot image (the "windows" option at the PXE menu), the guest machine has more than one virtual network adapter configured and operating, an error message will appear and the guest machine will not be able to enter the unprovisioned server list correctly.

Workaround: When performing OS provisioning using a DOS boot image, ensure that only one network adapter is configured or, alternatively, use a WinPE boot image.

Bug ID: 149729

Description: OS provisioning using authenticated windows share for media.

Subsystem: OS Provisioning

Platform: Windows

Symptom: You want to host your Windows media on a Windows 2000 server using a share. Access to the share is available to a local user on the server.

Example:

```
Server / Share:
\\servername\IOP
```

`user: username password: userpassword` is used to mount the share. Opsware Windows buildscript directories have the user hardcoded to `guest` with no password. Many security policies do not allow for a guest-enabled, read only share.

Workaround: Edit the file:

```
/opt/opsware/buildscripts/windows/buildserver.py
```

and replace these lines:

```
system_ini["network"]["username"] = self.mrl_username
system_ini["network"]["logondomain"] = self.mrl_domain
system_ini["network"]["workgroup"] = self.mrl_domain
```

with your share credentials. Also edit the following lines specifying the correct `username/password`:

```
# formulate net logon command line
                logonCmd = []
                logonCmd.append("lh %ramdrv%\\mslanman\\net")
                logonCmd.append("logon")
                logonCmd.append(self.mrl_username)

                logonCmd.append(self.mrl_password)
```

Bug ID: 159016

Description: Multimaster conflicts occur when customer changed by OS Sequence.

Subsystem: OS Provisioning Backend

Platform: Independent

Symptom: Boot a server to the server pool. Run an OS Sequence on the server during which the customer is changed by the OS Sequence from “Not Assigned" to "OS Prov". Following a successful OS Provisioning, deactivate the server. Reboot the server to the server pool and run an OS Sequence on the server where the customer is changed by the OS Sequence. A Multimaster conflict will occur during the OS Provisioning.

Workaround: There are two methods:

1. Set your customer either before or after OS provisioning and use the **Do not Change Customer** option.
2. Always initiate OS Provisioning from the same facility to which the machines are assigned. In the case of a satellite, run the job from the nearest facility.

Bug ID: 164220

Description: `TwistException` seen while creating RH4 OS profile and a new entry of OS profile is created which is incomplete.

Subsystem: OS Provisioning Backend

Platform: Red HAt Linux

Symptom: Import of a `Kickstart.cfg` file while creating a new OS Profile under Red Hat Linux AS4 fails with the error:

```
ImportError: libpopt.so.0: cannot open shared object file: No
such file or folder.
```

due to the missing package `popt-1.9.1-9_nonptl.i386.rpm`. A similar error occurs due to the missing package `libxml2-2.6.16-10.i386.rpm`.

Workaround: Install the `popt-1.9.1-9_nonptl.i386.rpm` and `libxml2-2.6.16-10.i386.rpm` packages and retry the operation.

Patch Management for Unix

Bug ID: 138929

Description: When you uninstall base fileset and update fileset in a single job, only the base fileset shows in the result and it cannot be uninstalled

Platform: AIX 5.3

Subsystem: SAS Client - Patch Management for Unix

Symptom: If you attempt to use the Patch Remediate feature to uninstall the base fileset and update fileset on the AIX 5.3 operating system in one remediation job, the install base fileset and its update should both be uninstalled. In the particular case, when uninstallation of base fileset fails, the error message is not clear enough to indicate the reason, and the update fileset is not mentioned in the error messages.

Workaround: None

Bug ID: 139208

Description: Using Patch Remediation to install ML01 on AIX 5.3 server produces some errors.

Platform: AIX 5.3.

Subsystem: SAS Client - Patch Management for Unix

Symptom: In some cases, using the Patch Remediation feature to install ML01 on AIX 5.3, the job will complete but with errors.

Workaround: None

Patch Management for Windows

Bug ID: 132400

Description: You have a server running Service Pack 3. When you try to remediate a patch policy that contains patch1 (for SP3), patch2 (for SP4), and Service Pack 4, only patch1 and Service Pack 4 will be installed. Since patch2 is intended for SP4, it will not get installed because when you start the remediate process, the server is still at SP3. After the first remediate is complete and you run the remediate process again, patch2 will then get installed.

Platform: Windows

Subsystem: Opsware SAS Client - Patch Management for Windows

Symptom: You have a patch policy attached to a server running Service Pack 3. The patch policy contains patch1 (for SP3), patch2 (for SP4), and Service Pack 4. When you run the remediate process, only patch1 and Service Pack 4 are installed. After the remediate process is complete and you run the remediate process again, patch2 will then get installed.

Workaround: If a Service Pack or a patch that is dependent on a certain Service Pack needs to be installed, install it manually. Do not use the remediate process to install a patch or a Service Pack that is dependent on a certain Service Pack.

Bug ID: 132415

Description: Email notifications were not sent when the install, uninstall, or remediate process failed due to pre-install or pre-uninstall scripts that failed to run.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: You tried to install a patch where the pre-install or pre-uninstall script failed. No email notifications were sent.

Workaround: None

Bug ID: 132467

Description: You cannot use the SAS Client to uninstall a patch that was installed with the OCC application node.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: You created an application node and added a patch to it. In the OCC, you installed the application node on a managed server. In the OCC, you removed the application node from the server. In the SAS Client, you tried to uninstall it with the Uninstall Patch task window and received an error explaining that “This patch cannot be uninstalled because it is referenced by another part of the model.”

Workaround: Use the SAS Client for all Windows patching.

Bug ID: 132599

Description: In the Properties view that lists patches for a certain Windows operating system, a patch is displayed as grayed out when Patch Management cannot determine whether the version of the patch that is installed is the same as the version of the patch that is in the Library. This occurs when the GUID identifier is not provided or is the same for both versions of the patch.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: A patch install appears successful; however, after verification, Opsware determined that the patch was not actually installed. When you view patches listed for a certain operating system in the Properties view, you see two patches displayed: one is grayed out and shown as installed-not-by-opsware and one is not installed.

Workaround: None

Bug ID: 132866

Description: When you add an Update Rollup to a patch policy, not all versions of it are added. Only the Update Rollup you selected will be added.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: You tried to add all versions on an Update Rollup to a patch policy. Only the version of the Update Rollup you selected was added.

Workaround: Manually add all versions of the Update Rollup to a patch policy.

Bug ID: 138063

Description: Unable to Access Patch Install/Uninstall, Patch Policy Install Jobs created prior to 6.x When Upgrading to 6.x.

Platform: All

Subsystem: Patch Jobs - Upgrade

Symptom: If you are upgrading a core to Opsware SAS 6.x, any Patch Install/Uninstall and Patch Policy Install jobs created prior to SAS 6.x will not be accessible. Attempting to open the pre-6.x jobs will fail.

Workaround: None

Bug ID: 164237

Description: **Import from Vendor** fails on **Opsware Admin** page.

Platform: Independent

Subsystem: SAS Client - Patch Management for Windows

Symptom: Import from Vendor fails with the error:

```
Communication with the Data Access Engine failed.
Details: Unbuffered entity enclosing request can not be
repeated.
```

Workaround: You can upload the MBSA patch database using the `populate-opsware-update-library` script.

Remediation

Bug ID: 152990

Description: Remediate preview is missing Windows patches that must be installed.

Subsystem: Remediation – Preview

Platform: Windows

Symptom: 6.5.1 fixed issues caused by Microsoft releasing patches for the same platform while using the same filenames. The fix involved changing how patch RoleClass records are created for each patch. A migration script to clean up existing patch RoleClasses was not included.

Workaround: On the server in your Multimaster Mesh that hosts the Data Access engine, log in as root and run:

```
# export LD_LIBRARY_PATH=/opt/opsware/lib
# /opt/opsware/bin/python /opt/opsware/spin/util/fix_6.6_data/
bz152990.pyc
```

SAS Client

Bug ID: 133253

Description: Actions available for the search results are not accurate if multiple windows are open in the SAS Client.

Subsystem: SAS Client - Search

Platform: Independent

Symptom: After performing a search in the SAS Client, If you open multiple windows and select objects in more than one window, then the actions available for the search results from the Action menu for the selected objects may in incorrect in the other windows.

Workaround: To display the exact options in the Action menu for the search results, reselect the objects in the active window and then select **Actions** from the **File** menu.

or

Right-click on the selected object and use the context menu to select the appropriate action.

Bug ID: 138720/134581

Description: SAS Client search does not display accurate results when you include special characters such as comma (,) in the value field.

Subsystem: SAS Client - Search

Platform: Independent

Symptom: In the SAS Client search, if you perform an Advance Search using the following values in the value field, the displayed search results are not accurate.

Value = special characters such as comma (,).

Workaround: Searching for comma value using the “begins with”, “ends with”, or “contains” comparison operator and a piece of the data that doesn't include the comma.

Bug ID: 139533

Description: Package window intermittently fails to open correctly in the SAS Client search feature.

Subsystem: SAS Client - Search

Platform: Independent

Symptom: When you double click on a package to open the Package window from the search results in the SAS Client, the Package window may display incomplete information. This behavior is observed intermittently.This behavior is observed intermittently.

Workaround: To open a Package window from the search results, select the Open menu item from the Action menu.

Bug ID: 138334

Description: Job Type drop-down list for both Job Logs and Recurring Schedules may not display correct available jobs if a user's permissions change while the SAS Client is open.

Platform: Independent

Subsystem: SAS Client - Jobs and Sessions

Symptom: Depending on when a user's granted permissions change, for example, while the user is logged in to the SAS Client, the Job Logs and Recurring Schedules Job Types drop-down list may not display the available job types accurately for that user. For example, if a user has permission to view all job type when the user starts the SAS Client, but during the session has a change in permissions that allow the user to not view certain job types, the Job Type drop-down list will still display all jobs as being available to view by the user.

Workaround: Close and restart to the SAS Client, or open a new window in the SAS Client and check the Job Types drop-down list again.

Bug ID: 144239

Description: When you close the remediate preview window while the process is still running, the Agent will get locked on the server and cannot run any remediate jobs.

Subsystem: SAS Client - Remediate

Platform: Independent

Symptom: When you launch remediate job from the server, run the preview, and then close the preview window while it is running, the Agent gets locked on the managed server and all other jobs fail. The following error message appears:

“The request to retrieve information from the Opsware Agent failed because it could not obtain a lock for the server. Most likely someone else is performing an operation on the same device. Try again in a few minutes. If the problem persists, please contact your Opsware Administrator.

Workaround: Wait for the remediate process to finish and then run the preview.

Bug ID: 144363

Description: Duplicating a device group from a device group without any rules, results in duplicate device group showing to contain servers.

Subsystem: SAS Client - Device Groups

Platform: Independent

Symptom: In the SAS Client you can duplicate a dynamic group which contains no rules and the resulting duplicate device group shows up in the device group list. In the navigation pane, when you select the duplicate device group, the members of the device group are shown in the Content pane.

Workaround: Create a rule for each dynamic device group or convert the dynamic device group to a static device group.

Bug ID: 145626

Description: Exceptions received when you update cache for patches.

Platform: HPUX and Solaris

Subsystem: SAS Client

Symptom: In the SAS Client when you select multiple patches and select Update Cache from the Tools menu, you receive an exception.

Workaround: None.

Bug ID: 149464

Description: Job Logs Filter May Appear Empty If User With View All Jobs Loses That Permission

Platform: Independent

Subsystem: Jobs

Symptom: If a user has View All Jobs permission and changes the Jobs user filter to another user, then that user then logs out and has their View All Jobs permissions revoked, the next time the user logs in to the SAS Client and views the job list, the user will not see any jobs.

Workaround:

1. If this situation occurs, have an administrator re-grant the user “View All Jobs” permission momentarily so that the user can remove the filter.
2. After the user removes the filter, they can have that permission revoked again and their list will show correctly.

SAS Client Reports

Bug ID: 133350

Description: Multi-byte characters do not display correctly in the chart legend.

Platform: Independent

Subsystem: SAS Client - Reports

Symptom: Characters that do not represent multi-byte characters display in the legend.

Workaround: Click the “Show all <nn> servers” link to view the correct multi-byte characters.

Bug ID: 133351

Description: No report results display when you click the multi-byte character link.

Platform: Independent

Subsystem: SAS Client - Reports

Symptom: When you click the multi-byte character link, no report results are displayed. The report should return the same number of objects as indicated in the link.

Workaround: Click the “Show all <nn> servers” link to view the correct multi-byte characters.

Bug ID: 133652

Description: Multi-byte characters do not display correctly in the report description.

Platform: Independent

Subsystem: SAS Client - Reports

Symptom: Logon to the NGUI. Run **Reports** > **Servers by Customer**. Select the Equals operator. Select a customer that has multi-byte character(s) in the name. Click Run. The characters `???` are displayed in the Report Description instead of the correct multi-byte character. Multi-byte characters are displayed correctly in the report output, but incorrectly in the report header.

Workaround: None. This occurs due to a bug in the BIRT report engine.

Bug ID: 134581

Description: The following special characters are not valid report parameters: #, $, %, &, +, and ;.

Platform: Independent

Subsystem: SAS Client - Reports

Symptom: There are no report results when you run a report that uses special characters in the report parameters.

Workaround: Select [Any Value] using the Equals operator or choose the Begins With, Ends With, or Contains operator and then enter a string for a wildcard search that contains everything up to the point of where the special character would be.

Bug ID: 136029

Description: The Action menu is disabled in Reports.

Platform: Independent

Subsystem: SAS Client - Reports

Symptom: When the Reports feature is selected in the navigation tree, the Action menu is disabled.

Workaround: Use the context-sensitive (right-click) menu.

Bug ID: 143410

Description: The SAS Client “Servers by Customer” report fails to return complete results on desktops with less than 1 GB MB RAM and when the number of servers is greater than 1000.

Platform: Windows

Subsystem: SAS Client - Reports

Symptom: In the SAS Client, if you run the following report, Server **Reports ➤ Servers by Customer**, the report takes a long time to complete on machines with less 512 MB RAM and

when you attempt to run the report on more than 4000 servers. Moreover, the report will not export to CSV – only the first few hundred records will be exported.

Workaround: To run this report, it is recommended that the system from which you are running the report has at least 1GB of memory, and you limit the number of servers to 1000.

If the report completes, export the report to HTML. Then, open the report in a Web browser, select all and then copy. Then, open Excel, select the whole sheet then perform an **Edit ➤ Paste**.

Bug ID: 147275

Description: The process of exporting some of the Compliance reports to HTML, XLS or PDF format does not work consistently.

Subsystem: SAS Client - Reports

Platform: Independent

Symptom: You tried to export the following reports to HTML, XLS, or PDF format but no files were generated: Software Compliance: Server by Policy, Server Software Policy Compliance, Server Software Policy Compliance Detail, Patch Compliance: Server by Policy, Server Patch Policy Compliance, and Server Patch Compliance Detail. The following error was displayed:

```
SEVERE java.net.SocketException: Connection reset
```

Workaround: None.

Bug ID: 147624

Description: In the Reports feature, the Remote Terminal connects to the wrong server.

Subsystem: SAS Client - Reports

Platform: Independent

Symptom: Run the Server by Customer Report. Select a Unix server in the report and launch a Remote Terminal to it. Exit out of the Remote Terminal and sort the list by selecting “customer”. Select a different server, right-click, and then select a Remote Terminal. This action will take you to the previously-selected (wrong) server.

Workaround: You must first left-click to select a row and then right-click so that an action in the **Option** menu correctly applies to the selected object.

Bug ID: 147274

Description: Slight delay when loading report parameters

Platform: Independent

Subsystem: SAS Client - Reports

Symptom: In some cases, when you first select a report in the SAS Client from the navigation pane, it may take a few moments for the report parameters to display.

Workaround: None

Bug ID: 148748

Description: In the Software Compliance reports, the Scan Software Compliance option in the right-click menu was enabled even though the user does not have permission to issue this scan.

Subsystem: SAS Client - Reports

Platform: Independent

Symptom: You belong to a user group that has no permission for Software Policy Management. In both the NGUI server manager and the Dashboard, the Software Compliance Scan would either be disabled or not available, as expected. However, when you run the Software Compliance Servers by Policy report, the Server Software Policy Compliance report, or the Server Software Policy Compliance Detail reports, and then right-click on a server, the Scan Software Compliance option is enabled. If you select this option, you will get a `fido.AuthorizationDeniedException` error. This option should be disabled if you do not have the required permissions.

Workaround: None.

Bug ID: 150436

Description: Non-compliant patches by server report results with “Patches not contained in Policies” not viewable.

Platform: Any

Subsystem: SAS Client Reporting - Compliance - Patch Policies

Symptom: If you run the SAS Client compliance report named Non-compliant Patch policies by server, in the results you may see an item named “Patches not contained in Policies” which shows a patch icon. If you attempt to double-click or right-click on this item, nothing will happen (it will not invoke a browser window or context window) because “Patches not contained in Policies” is not a real patch policy; it is just an indicator of patches not in policies that are relevant to the server.

Workaround: None

Bug ID: 149277

Description: An error occurs when running the Server Audit Compliance Detail Report.

Subsystem: SAS Client - Reports

Platform: Independent

Symptom: When you ran the Server Audit Compliance Detail Report using the default parameters, the report returned a large amount of data, such as more than 20,000 rows of data. Since this exceeds the amount of data that can be displayed, the following error was displayed:

```
org.eclipse.birt.report.service.api>ReportServiceException:
Error.
```

Workaround: Re-run this report with filters in place.

Bug ID: 149277

Description: Exported report shows different time than the time the report is generated

Platform: Any

Subsystem: SAS Client - Reports

Symptom: When you export a report in the SAS Client, the time that you will see marked on the exported report will be the time when the report was exported, not the time when the report was generated.

Workaround: None.

SAS Installer

Bug ID: 138694

Description: Upgrade failed due to an Oracle database problem.

Subsystem: Opsware Model Repository

Platform: Independent

Symptom: Oracle installs a SYS.AUDIT_ACTIONS table with the default synonym AUDIT_ACTION. During Opsware SAS installation of the Model Repository, the installer creates the TRUTH.AUDIT_ACTIONS table, and changes the synonym to TRUTH.AUDIT_ACTIONS. If you later upgrade your Oracle software, Oracle recreates the synonym as SYS.AUDIT_ACTIONS.

Workaround: If the AUDIT_ACTIONS synonym is overwritten by an Oracle upgrade, enter the following commands:

```
Su - oracle
Sqlplus "/ as sysdba"
Grant create session to truth;
Connect truth/<password>
Create or replace public synonym audit_actions for audit_
actions;
```

Bug ID: 140512

Description: Gateway startup does not detect when the `ConnectionLimit` parameter is set to a value that is higher than the operating system supports.

Subsystem: Opsware Gateway

Platform: Independent

Symptom: If the `ConnectionLimit` setting is larger than the maximum number of open file descriptors (`ulimit -n`), then the gateway may run out of file descriptors and fail. The default `ulimit` on Solaris is 256, the default `ulimit` on Linux is 1024. The default number of connections in the gateway is 900.

Workaround: Opsware recommends setting the `ulimit` on the operating system to 1024 or higher.

SAS Web Client

Bug ID: 136366

Description: TimedOutException occurs when deleting a dynamic server group containing many servers.

Subsystem: SAS Web Client

Platform: Independent

Symptom: In the SAS Web Client, when you delete a dynamic server group containing many servers, the following exception occurs:

```
Error Summary
Name:   Standard 500 Error
Description:    500 Internal Server Error
More Details...
Hide Details
Message Text:   Transaction Rolledback.; nested exception is:
weblogic.transaction.internal.TimedOutException: Transaction
timed out after
243 seconds
```

In spite of the exception, the dynamic server groups are deleted successfully.

Workaround: None

Bug ID: 148022

Description: An IP range cannot be used to automatically associate a server with a customer during deployment.

Platform: Independent

Subsystem: Opsware SAS Client - Environment

Symptom: In Opsware SAS 5.x and earlier, when a managed server first registers with a core, a customer can be associated with the server if the server is within the IP range for that customer. However, this automatic association does not work if the managed server contacts the core through an Opsware Gateway, which is the case for Opsware SAS 5.x and later. The Opsware SAS Policy Setter's Guide mistakenly tells the reader that associating servers with customers through the use of IP ranges still works.

For more information on this bug, see the description for bug ID 132880.

Workaround: Assign the customer to the managed server after deployment.

Software Management

Bug ID: 133443

Description: Bulk package upload can cause the "Package Type Not Defined in Truth" error.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: Import media uploads packages to the Software Repository. The Software Repository connects to the Data Access Engine to retrieve information specific to the package type being uploaded. Even though all packages uploaded during this step are of the same type, the call to the Data Access Engine will occasionally produce the following error: "Error uploading package. SUNWceax: Package Type Not Defined in Truth".

Workaround: None.

Bug ID: 136715

Description: In the SAS Client, you are unable to refresh the Package window.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client, if you have the Package window open and you make any changes to the servers associated with the packages in the Server window, then the changes made to the server are not reflected in the Package window when you refresh the Package window.

Workaround: Close the Package window and open it again.

Bug ID: 137989/138896

Description: Modifying the folder permissions in the SAS client does not reset the menu options in the Action menu immediately.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client, when you modify the folder permissions, the permissions are saved but the changes are not propagated to the menu options in the Action menu immediately.

Workaround: After you modify the folder permissions, select Update Cache from the Tools menu to propagate the changes to the menu options in the Action menu.

Bug ID: 138934

Description: The software compliance status for a non adoptable Solaris patch in a software policy is always “Not in Compliance”.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: If a software policy contains an non adoptable patch such as Solaris patch, then after remediating a server with the software policy, the compliance status displayed for the sever is always “Not in Compliance”.

Workaround: None.

Bug ID: 139254

Description: Folder objects such as packages and software policies can be moved to another location, even if you don't have Read or Write permissions for those objects.

Platform: Independent

Subsystem: Software Management

Symptom: If you have Write permission on a folder, and No Read or Write permissions on the objects (such as packages, software policies) contained in the folder, then you can view the packages and software policies in the folder. You will not be able to perform any actions on the Folder objects. If you move or cut/paste the folder to another location, then the packages and software policies in the folder will also be moved or cut and then pasted to the destination folder.

Workaround: None.

Bug ID: 139040

Description: Install Software Policy Template fails on managed servers belonging to multiple platform families.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: When you install a Software Policy Template on managed servers belonging to multiple platform families, and if the selected software policy template's platform family does not match the platform family of the managed servers, an exception occurs and the Software Policy Template is not attached to the managed servers.

Workaround: None. When you install a software policy template on managed servers, the software policy template and the managed servers must belong to the same platform family.

Bug ID: 139046

Description: Unable to delete HP-UX depot patches in the SAS Client.

Subsystem: SAS Client - Software Management

Platform: HP-UX

Symptom: After you import a HP-UX depot patch to Opsware SAS, you are unable to delete the package immediately from the SAS Client. Deleting the package results in the following error:

```
"Uabled to delete item because it is either in use or you do not
have sufficient privileges"
```

This behavior is only observed if the HP-UX depot patch is not located in a folder.

Workaround: To delete a HP-UX depot patch immediately after importing it to Opsware SAS, perform the following steps:

1. Delete the HP-UX depot patch using SAS Client.
2. From the Tools menu, select Update Cache.
3. Select the HP-UX depot patch in the SAS Client and delete it again.

Bug ID: 138400

Description: Software is not uninstalled after a migrated software policy is detached and remediated from a server

Platform: Independent

Subsystem: Software Management ➤ Content Migration

Symptom: If you detach a migrated software policy from a server and remediate, the packages are not removed from the server.

Workaround: You can install software by using a migrated software policy in the SAS Client but you cannot uninstall software until you have completed the migration. You must complete migration as soon as possible and do not remediate servers or detach software policies unless you have completed migration.

Bug ID: 141459

Description: The SAS client stops responding when you attach a policy to several servers.

Platform: Independent

Subsystem: SAS Client - Software Management

Symptom: In the SAS client when you attach a policy to several servers the SAS client stops responding.

Workaround: None.

Bug ID: 143642

Description: Remediating an RPM package to a server in one core immediately after importing the package in another core in a multimaster mesh fails with metadata missing error.

Platform: Independent

Subsystem: SAS Client - Software Management

Symptom: In a multimaster mesh, after importing an RPM package in one core, if you try to install the package in another core immediately, then the remediation fails with metadata missing error.

Workaround: If you receive this error immediately after importing an RPM in one core and then attempting to install the RPM on a server in another core, wait several minutes, then retry the operation.

Bug ID: 143751

Description: Uninstall fails for zope packages on SLES 10.

Subsystem: SAS Client - RPM Deployment

Platform: Linux

Symptom: In the SAS Client, when you try to uninstall a zope package on SLES 10 server by remediating the server with a software policy containing zope package, the remediate process fails with the following error:

```
ImportError: /opt/zope/lib/python/ZODB/cPersistence.so: wrong
ELF class:
ELFCLASS32
..failed
error: %preun(zope-2.7.8-15.i586) scriptlet failed, exit status
Software uninstall failed with an exit code of 255
```

Workaround: To uninstall a zope package on a SLES 10 server, add “--noscripts” to the uninstall properties of the zope package in the Package Properties window before remediating the server.

Bug ID: 144220

Description: Performance issues when remediating a policy containing a large number of RPMs.

Subsystem: SAS Client - RPM Deployment

Platform: Linux

Symptom: When remediating a policy which contains a large number of RPMs, the SAS Client does not appear to be performing any action.

Installing RPMs contains consists of three phases.

Phase 1: Resolve dependencies for the RPMs contained in the policy.

Phase 2: Download the RPMs resulting from phase 1.

Phase 3: Install the RPMs.

Phase 1 corresponds to the “Preview” step of remediating a policy.

Even if the “Preview” button is not clicked, this phase must still be performed. While this phase is occurring, the SAS Client does not provide any feedback. If many RPMs (more than one hundred) are involved, this step can take up to 45 minutes to complete. Although nothing appears to be happening in the SAS Client, in reality, Opsware is performing the steps needed to resolve dependencies. Because this phase involves many transactions between the managed server and the SAS core, the operation is not instantaneous.

Workaround: None.

Bug ID: 144301/144379

Description: To authenticate with Opsware, the `rhn_import` script requires to access the Command Engine or the Data Access Engine certificate or the user name and password stored in the Configuration file.

Subsystem: SAS Client - RPM Deployment

Platform: Independent

Symptom: There are two ways in which rhn_import authenticates with Opsware: Command Engine or the Data Access Engine certificate or via user name and password stored in the Configuration file in the Software Repository.

To run the `rhn_import` successfully, the script needs to either access to the Command Engine or the Data Access Engine certificate or the configuration file should contain the `uapi_user=Username` and `uapi_pass=Password` options.

If the Command Engine or the Data Access Engine is not installed on the same server as the Software Repository then the certificate may not be installed in the server containing the Software Repository. Hence the rhn_import may fail if the configuration file does not contain the `uapi_user=Username` and `uapi_pass=Password` options.

Workaround: In case certificate is not available, then specify the `uapi_user=Username` and `uapi_pass=Password` options in the Configuration file.

Bug ID: 144719

Description: Adding packages to a software policy may result in null pointer exception.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client, when you create a software policy from the Library > By Folder view and then immediately try to add packages to the software policy, you may receive a null pointer exception. This behavior is observed intermittently.

Workaround: Close the Software Policy window and re-open the Software Policy window to add the packages.

Bug ID: 145246

Description: Unable to delete a build customization script in the SAS Client.

Platform: Independent

Subsystem: SAS Client - Software Management

Symptom: In the SAS Client, if you delete a build customization script package, the package is not deleted.

Workaround: Restart the SAS Client to delete the package.

Bug ID: 146298

Description: Editing the /Opsware/Tools folder in the Library in the SAS Client may result in errors.

Platform: Independent

Subsystem: Software Management

Symptom: As an Administrator user, editing the /Opsware/Tools folder in the Library in the SAS Client may result in the following:

Inability to install RPMs
Inability to remove RPMs
Inability to upgrade RPMs

Workaround: Do not edit the /Opsware/Tools folder in the Library

Bug ID: 147577

Description: Write permission is required to copy a folder in the Software Library.

Platform: Independent

Subsystem: Software Management

Symptom: You are unable to copy a folder to another location if you do not have Write permission to the source folder. You also require Write permission for the destination folder.

Workaround: To copy a folder to another location, you require Write permissions to the source folder and the destination folder.

Bug ID: 148745

Description: Pre or Post install scripts specified for HP-UX Products are not executed on the managed server during remediation.

Platform: Independent

Subsystem: Software Management

Symptom: For HP-UX products, if you specify any pre or post install scripts on the Package window and then add the HP-UX package to a software policy and remediate the server, then the HP-UX packages are installed successfully, but the pre or post install scripts are not executed on the server.

Workaround: None.

Bug ID: 148771

Description: After upgrading to SAS 6.5.1, Software Compliance Scan was disabled for users in the Advanced Users Group. This behavior continues in 6.61.

Platform: Independent

Subsystem: Software Management

Symptom: After you upgraded to SAS 6.5.1, the Software Compliance Scan functionality was disabled for users in the Advanced Users Group in the SAS Client. This behavior continues in 6.61.

Workaround: Perform the following steps to enable the Software Compliance Scan functionality in an upgraded core:

1. In the SAS Web Client, log on as admin, select the Advanced Users Group and unassign any one of the Software Policy permission.
2. Save this permission change of the Advanced Users Group.
3. Reassign back the same Software Policy permission to the Advanced Users Group. Save this change
4. From the SAS Client, log off the user in Advanced Users group and then re-log on with the same user.

In the SAS Client, the Software Compliance Scan functionality is now enabled for the users in the Advanced Users Group.

Bug ID: 148777

Description: Selecting the Control Parameter step in the Run ISM Control window from the Run ISM Control job leads to an error.

Platform: Independent

Subsystem: Software Management

Symptom: In the SAS Client in the Job Logs window, when you open a Run ISM Control job, the Run ISM Control window appears. Selecting the step “Control Parameters” in this window leads to the following error:

“Twist exception while getting parent folder”

Workaround: Close the error message to continue navigating through the other steps in the Run ISM Control window.

Bug ID: 148797

Description: Compliance status of a managed server does not get updated after remediation, if the server is in the destination core in a multimaster mesh.

Platform: Independent

Subsystem: Software Management

Symptom: In a multimaster mesh, if the managed server is in a remote core, in other words, the SAS Client is connected to a different core, then when the managed server is remediated with a software policy, the compliance status may not reflect the correct result. But the software resources specified in the software policy are installed on the managed server.

Bug ID: 149043

Description: Unable to install both the versions of an RPM package on RHEL 32-bit server.

Platform: Red Hat Linux

Subsystem: Software Management

Symptom: On RHEL 32-bit server, using Opsware SAS you can install only one version of an RPM package. You can either install a .i386 or .686 version of an RPM package. If an RPM package is already installed on a RHEL 32-bit server and then if you try to remediate the server with a software policy containing the same RPM package (but both the versions: .i386 and .686), then the RPM package is not installed on the server and the compliance status of the server becomes non-compliant.

Workaround: None.

Bug ID: 149093

Description: Exporting multiple packages with the same name in the SAS Client overwrites the packages.

Platform: Independent

Subsystem: Software Management

Symptom: When you export multiple packages with the identical name to the software library in the SAS Client, then the packages are overwritten and only one package is exported to the folder in the software library.

Workaround: None.

Bug ID: 157932

Description: The Client doesn't show the default ISM tool software policy when you attach it to a server.

Platform: Independent

Subsystem: Software Management

Symptom: When you attach an ISMtool software policy in the `/Opsware/Tools/ISMtool folder` to a device, the UI does not present the ISMtool policy in the pick list.

Workaround: Navigate to the `/Opsware/Tools/ISMtool` folder in the **Library By Folder** tab, then attach the policy to the device. The second attachment of the software policy to the device UI should cause the ISMtool policy to appear in the pick list.

Bug ID: 160891

Description: A staged job with a combined immediate download and scheduled install displays a status of continuous even when completed.

Platform: Independent

Subsystem: Software Management

Symptom: For example:

1. Launch Remediate
2. Select **Staged.**
3. Schedule for a combined **Download Immediately** and **Install**.
4. Start the job.
5. When the download is complete but the install is still pending, reopen the job from the job log.

The job status displays as **Continuous**. There are situations in which it is not possible to determine the status of a job. In the above case, a staged job with Immediate Download and scheduled install can be interpreted as either Staged or Continuous and there is currently no way to differentiate between the two.

Workaround: None

Bug ID: 164366

Description: Software policies are not visible until you have browsed to/opened them from within their folder structure.

Platform: Independent

Subsystem: Software Management: UI - Library

Symptom: Login to SAS client, select a server from **Devices** and right click **Install Software**. In the **Install Software** window certain Software Policies may not be displayed. Navigate through the Folder library structures and open and close the policy that is not being displayed, the policy will then be visible in the **Install Software** window when you next reopen it.

Workarounds:

- Navigate through the Folder library structures and open and close the policy that is not being displayed, the policy will then be visible in the **Install Software** window when you next reopen it.
- Do a search for all policies using the search feature.
- Visit the by type views for each platform of interest for the folder object type.
- Open each folder that stores the policies.

Virtualization

Bug ID: 143998

Description: Virtualization View is Not Refreshed Automatically When Modifying (Starting, Stopping, or Deleting) a Zone

Platform: Independent

Subsystem: Virtualization - Refresh for Zone Changes

Symptom: When you modify a zone in the SAS Client (Devices ➤ Virtual Servers), such as stopping, starting, or deleting a zone, the contents pane will not automatically refresh the view to reflect the new state (or absence) of the zone. For example, if you were to delete a zone, the zone will still appear until you manually refreshed the window.

Workaround: When you modify a zone (start, stop, delete), from the **View** menu, select **Refresh** (or press F5)

Bug ID: 160839

Description: Newly provisioned Solaris 10 x86 VM is shown as an unmanaged VM.

Platform: Solaris

Subsystem: Virtualization UI

Symptom: In Virtualization Director, select Create VM with OS provisioning for Solaris 10 x86 VM. After the VM was created, select **Servers ➤ Virtual Servers**. The newly created VM was displayed as an unmanaged VM. Its Hostname was blank, and its Virtual Machine Name was that of the host ESX 3 server. In 6.6, managed Solaris 10 VMs are now displayed with a managed server icon in **Devices ➤ Virtual Servers**. However, the managed server views Summary, Properties, Hardware, Custom Attributes, Group Membership, History, and Compliance are still empty in **Devices ➤ Virtual Servers**. These views are populated correctly in **Devices ➤ All Managed Servers**.

Workaround: None

Visual Application Manager (VAM)

Bug ID: 143148

Description: HP-UX Process Family Limitation

Platform: HP-UX

Subsystem: Visualizing Process Families for HP-UX

Symptom: VAM currently is unable to report environment variables, command line, and current working directory for processes running on HP-UX.

Workaround: None.

Visual Packager

Bug ID: 139169

Description: Unable to package and deploy unreadable/inaccessible Windows Registry keys

Platform: Windows

Subsystem: Visual Packager

Symptom: If you attempt to package Windows Registry objects that are either unreadable or inaccessible by Opsware SAS, the objects will not package completely and will not be available for copying to a target server or remediate as a package in a software policy.

Workaround: Make sure that the Windows Registry key you are trying to package are readable. If you attempt to package a non-readable Windows Registry key, you will see an error message in the Java console.

Bug ID: 139506

Description: Visual Packager supports only ASCII characters in the software policy name.

Subsystem: SAS Client - Visual Packager

Platform: Independent

Symptom: If you include non-ASCII characters in the software policy Name in the Create Package window, Visual Packager creates a new software policy in the folder hierarchy (with packages attached) and each non-ASCII character displays as a question mark (?).

Workaround: None. Do not include non- ASCII characters in the software policy name.

Bug ID: 143744

Description: Unable to create a package using Visual Packager on AIX.

Platform: AIX

Subsystem: SAS Client - Visual Packager

Symptom: Using Visual Packager when you create a package on AIX and include filesystems or Installed Patches in the Selection field, then the create package process fails with the following error:

```
com.opsware.common.LegacyException: msg= java.io.IOException:
Executing
command to package contenton server on server 390001
```

Workaround: None.

Bug ID: 143744

Description: Creating package with supplied fileset for UpdateFileset (patch) fails.

Platform: AIX

Subsystem: Visual Packager Backend

Symptom: When creating an AIX package with Visual Packager, select an install patch that has an update fileset and then try to create the package. Result:

```
com.opsware.common.LegacyException:  msg= java.io.IOException: 
Executing command to package contenton server on server <server-
id> ...
```

Workaround: First import the LPP into SAS and then create a policy via Visual Packager that involves inner/child packages of the LPP.

Bug ID: 149117

Description: In the Create Package window, you can view all the COM+ objects with unregistered DLLs.

Platform: Independent

Subsystem: Visual Packager

Symptom: The Visual Packager feature allows you to use the Create Package window to see COM+ objects with unregistered DLLs and create a package with those COM+ objects. But when you attempt to install the package on a server, the remediate job will run successfully, but the COM+ objects will not get installed on the target server.

Workaround: To install COM+ objects with unregistered DLLs, perform the following steps:

1. Register the DLL on the source server.
2. Create a package with the COM+ objects.
3. Attach the software policy to the server.
4. Remediate the server.

Chapter 6: Documentation Errata

IN THIS CHAPTER

This chapter contains the following topics:

- Update to the Opsware® SAS Planning and Installation Guide
- Update to the Opsware® SAS User’s Guide: Application Automation
- Updates to the Opsware SAS 6.5 User’s Guide: Server Automation
- Updates to the Opsware SAS 6.5 Content Migration Guide

Update to the *Opsware® SAS Planning and Installation Guide*

Chapter 7: Post-Installation Tasks

The note on page 133 of the *Opsware® SAS Planning and Installation Guide* states:

“You need to install only one Windows Agent Deployment Helper for each Opsware core.”

This should read:

"You can install no more than one Windows Agent Deployment Helper in each Opsware mesh."

Chapter 8: Multimaster Installation

When installing the Multimaster Components to upgrade a core from standalone to Multimaster, you must shut down all running components, start the Opsware Gateway (`opswgw-cgw0`), install the Multimaster Components, then run the Opsware start script to start all components. Previous versions of the *Opsware® SAS Planning and Installation Guide* omitted the step to stop all components before upgrading to Multimaster. The Opsware SAS 6.6 Planning and Installation Guide includes this phase.

Update to the *Opsware® SAS User's Guide: Application Automation*

Chapter 9: Operating System Provisioning, Red Hat Linux Support

Under the heading "Supported Operating Systems for OS Provisioning," the OS Provisioning feature also supports installation of the following versions of Red Hat Linux in addition to those already listed:

- Red Hat Enterprise Linux Server 5 (x86 and x86_64)
- Red Hat Enterprise Linux Desktop 5 (x86 and x86_64)

Updates to the Opsware SAS 6.5 User's Guide: Server Automation

The followings topic is new for the Opsware SAS 6.5 User's Guide: Server Automation:

Executing My Scripts or Shared Scripts

Step 10 in the section "Executing My Scripts or Shared Scripts" should include the following information:

In the SAS Web Client, you can run the *Shared Scripts* only as root and you must have the appropriate permissions to run the Shared Scripts as root. You can run the *My Scripts* as either root (if you have the appropriate permission) or as a specified user.

Updates to the Opsware SAS 6.5 Content Migration Guide

The following topic is new for the Opsware SAS 6.5 Content Migration Guide:

Supported Operating Systems for Managed Servers

For a complete list of the supported operating systems for Opsware Agents and the SAS Client in Opsware SAS, see the section "Supported Operating Systems for Managed Servers" in the Opsware SAS 6.6 Release Notes.