Opsware® SAS 6.6 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: What's New in Opsware SAS 6.6

IN THIS CHAPTER

This chapter contains the following topics:

Opsware Server Automation System (SAS) 6.6 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 6.6 release.

Support for HP-UX 11iv3 and Solaris 10 U4 Servers

You can now discover and add HP-UX 11iv3 and Solaris 10 U4 servers to your Managed Server Pool. All Opsware SAS management features are available including monitoring, OS provisioning, software monitoring, and so on.

Serial Number Retrieval for HP-UX, IBM AIX, and Sun Solaris Servers

Opsware SAS 6.6 provides improved retrieval of server serial numbers for HP-UX, IBM AIX, and Sun Solaris servers.

Remediation Performance Improvements

Many internal optimizations provide significantly improved remediation performance.

- Compliance checks on a per server basis.
- Alarm timeout in the opsware Command Engine for agent modules.
- Improved error handling.
- Memory handling Optimizations
- reduced number of calls to the Data Access Engine during Analyze.
- Many others.

OS Provisioning: Define Customer when Deploying a Sequence

When deploying a Sequence during OS Provisioning, you can now define a customer using the Run OS Sequence wizard. Previously you were required to define the customer separately and attach it to the Sequence.

Device Recalculation Improvements

Device group recalculation now give precedence to groups over attributes.

There are three new settings:

`twist.recalcevent.attrConversionMaxTime`

- Set in ms default value of 10000 (i.e.: 10 seconds). This is the maximum amount of time to be spent spend converting attributes.

`twist.recalcevent.maxDevices`

- The maximum number of devices that a group will recalculate. If more than that number of devices are polled, the event recalculation will be converted into an *initial* membership, a full recalculation across all possible devices. The default value is 500.

`twist.recalcevent.accessOnly`

- Values are TRUE|FALSE. If set to TRUE, causes a recalculation only of access groups.

Content Migration Improvements

Opsware SAS 6.6 provides improved content migration speed on large datasets and minimizes timeouts when using the DCML Export Tool (DET).

SAS Client Installer Bundled with Sun Java JRE 1.4.2_15

The Opsware SAS Client installer will install Sun Java JRE 1.4.2_15 during the Client installation process. This JRE installation is for use only with Opsware SAS and will not conflict with or overwrite your systems' default JRE installations.

Chapter 2: Platform and Environmental Support

IN THIS CHAPTER

This chapter contains the following topics:

- Supported Operating Systems
- Statement of Support for HP-UX on HP vPars and HPVM
- Supported Core Operating Systems
- Operating System Deprecation and End of SupportOperating System Deprecation and End of Support
- Supported Installations and Upgrades for Opsware SAS 6.6
- SAS Client Java Version
- Documentation for Opsware SAS 6.6

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
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 Family 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.

Statement of Support for HP-UX on HP vPars and HPVM

The HP Server Automation Business Unit confirms managed server support for HP-UX on HP vPars and HPVM technology.

Specifically, HP confirms that HP Server Automation versions 6.6, 7.5, 7.8 and later support the following as an equal to HP-UX support on individual physical systems:

- HP-UX 11i v2 & 11i v3 Integrity VM (HPVM) guests running on Integrity VM B.04.00 or later
- HP-UX 11i v2 & 11i v3 vPars running on vPars A.05.00 or later.

This support entails that, for the above supported HP-UX versions, all supported features are also supported on HP vPars and HPVM. The solution at this point does not have any support for creating, starting or stopping the vPars or HPVM virtual machines.

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 6.6:

- 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 6.6:

- 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 6.6

The Opsware SAS 6.6 release supports the following installations:

- Upgrading a standalone core from Opsware SAS 6.5.1 to 6.6
- Upgrading a multimaster mesh from Opsware SAS 6.5.1 to 6.6
- Upgrading an Opsware Satellite from Opsware SAS 6.5.1 to 6.6

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 6.6

This release comes with the following documentation:

- *Opsware SAS 6.6 Release Notes*
- *Opsware SAS 6.6 Upgrade Guide*
- *Opsware SAS 6.6 Planning and Installation Guide*

The following documentation is applicable to this release:

- *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 *6.6* are compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 6.6 features with Opsware Agent versions prior to 6.6 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 6.6

IN THIS CHAPTER

This chapter contains bugs that have a severity level of Critical or Major and are fixed in Opsware SAS 6.6. These descriptions are arranged by the following features:

- Agents
- Agent Deployment
- Application Configuration
- Command Engine
- Data Access Engine
- DCML Export Tool (DET)
- Global Filesystem (OGFS)
- ISM Tool
- Jobs and Sessions
- Model Repository
- NAS/SAS Integration
- Opsware Command Center (OCC)
- Opsware Installer
- OS Provisioning
- Patch Management
- Red Hat Network Import
- Server Management
- Software Management
- Virtualization

Agents

Bug ID: 149846

Description: HP-UX 11.31 agent fails to startup after installation.

Platform: Independent

Subsystem: Agent

Symptom: The agent installs properly on an HP-UX 11.31, but it fails to startup. This appears to be a Python 1.5 incompatibility.

Resolution: Fixed

Bug ID: 150316/134695

Description: OPSWrpm fails to calculate free space on a 5TB partition.

Platform: Independent

Subsystem: Agent

Symptom: OPSWrpm required an upgrade to be able to handle larger file systems.

Resolution: Fixed

Bug ID: 159508

Description: Agent does not report speed/duplex for unconfigured devices.

Platform: Independent

Subsystem: Agent

Symptom: RFE: Unconfigured devices have a link that can be polled for the `link_status`, `link_speed` and `duplex` using `ndd`. Make it possible to use the UAPI to retrieve this information and cross reference it to switches. Another use case: standby interfaces that are dynamically configured during failover operations. These standby interfaces can be properly configured (especially duplex) so that the failover results in a well-behaved configuration if the agent can retrieve this information.

Resolution: Fixed

Bug ID: 159699/150194

Description: Linux Agent reports half of CPUs.

Platform: Red Hat Linux

Subsystem: Agent

Symptom: Redhat Linux agents reports only half of the actual CPUs.

This affects Pentium 3 and Xeon processors. Agents appear to ignore any additional CPUs if CPUs have the same physical id or have Hyper-threading disabled.

Resolution: Fixed

Bug ID: 160622

Description: `netif` reports virtual interfaces as enabled=0 on SunOS 5.10

Platform: Independent

Subsystem: Agent

Symptom: Agents are unable to determine enabled/disabled status of a device separately from its static/dhcp status.

Resolution: Fixed

Bug ID: 161376

Description: Zip handler changes agent's cwd while extracting zip and doesn't restore it.

Platform: Independent

Subsystem: Agent

Symptom: Agents are designed to run with the `cwd` set to `/var/opt/opsware/agent`, but the zip handler is changes the `cwd` to that of the extraction directory for the zip file it is installing. If the zip file is later removed (which can remove the extraction directoryl), the agent may be left in a non-existent cwd causing later operations expecting the `/var/opt/opsware/agent` directory to fail.

Resolution: Fixed

Agent Deployment

Bug ID: 155526/148480

Description: Some agent assimilation actions using ADT lead to conflicts in the core.

Platform:

Subsystem: Agent Deployment/Upgrade Backends

Symptom: Scenario:

1. Initially server was showing as deactivated in one core and was actually assimilated to another core.
2. Removed agent manually from the managed server
   `cd /opt/opsware/agent/bin`
   run agent_uninstall.sh script
3. Assimilated the same server to a third core using ADT.
4. Server did not show in the third core but was still showing as deactivated in first core (an update cache did not help).
5. Deleted the server from the first core.
6. Removed agent again manually.
7. Re-assimilated server to the third core using ADT.

This time the agent showed only in the third core but it also created conflicts in the core.

Resolution: Fixed

Application Configuration

Bug ID: 151438

Description: Failure to push configuration on HP-UX v11.31.

Platform: HP-UX v11.31

Subsystem: Application Configuration Backend

Symptom: When pusing a configuration under HP-UX v11.31, the process would fail with an error similar to the following:


```
Failed to create snapshot: Input stream is not an unconstructed
snapshot.\012'}, 'faultCode': 101}, 'message': 'OpswareError:
serverCompliance.FailedToCreateSnapshot [ module:
com.opsware.compliance.server.rmi, method: createSnapshot,
line: 204,timestamp: 2007-07-06 22:12:31.077, msg:
java.io.IOException: Process failed:Gathering Filesystem
data\012Executing command to Snapshot filesystem on Server
130063\012Executing command failed\0121\012RuntimeError: Bad
magic number in .pyc file\012ERR: Failed to create snapshot:
Input stream is not an unconstructed snapshot.\012
```

Resolution: Fixed

Bug ID: 159272

Description: UAPI `startConfigurationPush` fails when there are more than 40 servers.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: UAPI appconfig async call `startConfigurationPush` fails after 30-40 servers (one job per server).

Each server after the first 30-40 fails after 10 minutes with the following error:

```
[['7990601L', ['OpswareError', {'hostname': 'None', 'timestamp':
'16/Nov/2007
195814', 'timeticks': '1195243094L', 'args': [], 'request':
'UNKNOWN',
'module': 'opsware.asynctwist~32g.0.3', 'cascade': 'None',
'faultCode': '101',
'tb_chain': [], 'been_cascaded': '0', 'error_name':
'wayscripts.commandTimeout', 'params': {}, 'line': '196',
'faultString':
'wayscripts.commandTimeout', 'method': 'getError'}]]]
```

For example:

```
for each server in (list of servers)
    for each instance in (list of instances)
        push instance to server
serverService.startConfigurationPush(new
ServerRef(serverId), instanceName, null, null,
null).getId();
```

Resolution: Fixed

Bug ID: 159604

Description: Application Configuration's use of `DevicesVO` leads to excessive calls to the Data Access Engine.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: When running an Application Configuration push against 100 servers, the Data Access Engine receives an excessive number of requests for realm information and bandwidth-to-core information.

Resolution: Fixed

Bug ID: 161078

Description: Fix `asynctwist` to use all Web Services Data Access Engines in the DC.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: Currently precedence is given to call backs to the originating Web Services Data Access Engine rather than allowing for alternatives. This negatively impacts performance in a multi box core.

Resolution: Fixed

Command Engine

Bug ID: 159122

Description: the Command Engine can be very slow when tagging large sessions as zombies.

Platform: Independent

Subsystem: Opsware Command Engine

Symptom: When the Command Engine tags a zombie session, it signs the entire session tree associated with the given session, including all child objects.

This can take an unacceptably long time.

Resolution: Fixed

Data Access Engine

Bug ID: 156886/157313

Description: `cogbot.swreg.ignore_apars` probably doesn't work with SP/CSPs.

Platform: IBM AIX

Subsystem: Data Access Engine

Symptom: Maintenance level patches not being ignored because of a change by IBM in nameing conventions.

Resolution: Fixed

Bug ID: 157042/160590

Description: `_AIXFilesetUnit.updateAFSUsWithSelf` can associate an AFSU with both a Base and Update FSU.

Subsystem: Data Access Engine

Platform: Independent

Symptom: The Data Access Engine should associate only a single file set (be it Base or Update) with each APARFilesetUnit.

Resolution: Fixed

Bug ID: 157521

Description: Device group recalculation should give precedence to groups used in access control.

Platform: Independent

Subsystem: Data Access Engine – Device Recalculation

Symptom: Groups that are in the queue as a result of an event, that are access control boundaries, should have precedence over everything with the possible exception of new group creation. See “Device Recalculation Improvements” on page 8.

Resolution: Fixed

Bug ID: 157523

Description: Heavy core usage can overload the group recalculation thread causing it not to process groups within a reasonable period of time.

Platform: Independent

Subsystem: Data Access Engine – Device Recalculation

Symptom: Because the Data Access Engine processes attributes before groups (in blocks of 100 attributes simultaneously), it's possible while under heavy load for the attribute pool to not become exhausted until long after the groups would be expected to be handled). See “Device Recalculation Improvements” on page 8.

Resolution: Fixed

DCML Export Tool (DET)

Bug ID: 149809

Description: DET (cbt) does not retry on Web Services Data Access Engine (twist) timeout

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: The Web Services Data Access Engine times out during a content import, the import fails, and does not attempt a retry.

Resolution: Fixed

Bug ID: 158250

Description: DET does not import OS Sequence remediate job arguments.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: When you export an OS Sequence and then import it into another mesh via the DET, the remediate job arguments (everything under **Tasks ➤ Remediate Policies**) are initialized as disabled.

Resolution: Fixed

Bug ID: 159256/159546/159845/160412

Description: Double quote problem re-introduced in `cbt-32h_0_0_8`.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: Create an OS that has a custom build script with quote characters in it, export the OS and then import it to a core. The quote characters are changed to `&quot`.

Resolution: Fixed

Bug ID: 159718

Description: CBT misc import fails.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: Export/import of PATCH_META_DATA units (Microsoft Patch Databases), import fails with an error:

```
INFO: (6%) Starting Importing Microsoft Patch Database: package
Oct 7, 2007 7:18:09 PM com.opsware.cbt.util.FileProgressListener
error
SEVERE: Importing Microsoft Patch Database: package Message:
OpswareError:
wordbot.xmlSyntaxParsingError [ module: server.py, method:
extractMetaInfoMbsa12, line: 4613, hostname:
usplsopmo002.opmodl1.elabs.eds.com, timestamp: 07/Oct/2007
191809 ]
```

```
OpswareError: wordbot.xmlSyntaxParsingError [ module: server.py,
method:
extractMetaInfoMbsa12, line: 4613 [remainder of error elided]
```

Resolution: Fixed

Bug ID: 159844

Description: `RPMUnit` display name does not change when unit is released or version is changed.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: When the `software_version` or `software_release` fields of a unit record change, the corresponding `unit_display_name` is not updated. For example, when importing a new version of a non-software repository RPM using DET.

Resolution: Fixed

Global Filesystem (OGFS)

Bug ID: 150002

Description: ROOT access to hub box available to anyone who has root access to a managed server.

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: Anyone able to get the `management_ip` of a server and who has `global_shell` access could get root access to the hub.

Resolution: Fixed

Bug ID: 153721

Description: `pam_sm_close_session` causes core dump when USERNAME environment variable is not set.

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: OPSWsshd fails on a segmentation violation causing a core dump.

Resolution: Fixed

Bug ID: 155143/156999

Description: OGSH connections causing kernel panic.

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: processes that create multiple parallel `ttlg` connections/ssh connections to the OGSH to execute various scripts could cause a kernel panic.

Resolution: Fixed

Bug ID: 159885

Description: The `ls -lR /opsw` command hangs and the hub becomes very slow.

Platform: Red Hat Linux AS 3

Subsystem: Global File System/Shell Backend

Symptom: The remount operation hangs and causes the hub to slow. Since running of hub inode cache triggers the remount operation when the size of hub inode cache reaches certain threshold (100000 inodes), the operation and failure can occur silently.

Resolution: Fixed

Bug ID: 159922/159923

Description: OGFS: memory leak in Hub

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: Two distinct sets of objects are being leaked in the Hub:

- The objects in equal proportions: caused by a a failed file system operation on an Agent.
- The objects in a 1:1:1:2:3 ratio: caused by excessive `DevicesVO` transactions.

Resolution: Fixed

Bug ID: 160225

Description: Post device change log and audit event messages in a separate thread.

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: Currently the Hub writes device change log and audit event message synchronously when processing Agent file system write operations (and ttlg requests). This adds to the elapsed time for these operations and impacts application performance (such as AppConfig).

A separate thread should be dedicated to writing these messages (much as the Opsware Command Engine writes commands back asynchronously to the Data Access Engine).

Resolution: Fixed

Bug ID: 160537

Description: OGFS: hang caused by stuck connection to managed server(s).

Platform: Independent

Subsystem: Global File System/Shell Backend

Symptom: An OGFS request gets stuck. When this happens, the request never completes (either successfully or with an error) with the following consequences on Linux (until an OGFS restart):

- The calling process hangs unkillably (linux only).
- A FUSE request slot is consumed (linux only).
- If the in-flight request was a lookup of a directory then all requests for the subtree at that directory will hang (linux and solaris).

The AgentProxy should shutdown the connection to the Agent if a request has been live for more than some threshold (which should be longer than the existing 120 second idle threshold).

Resolution: Fixed

Bug ID: 160476

Description: Ignored OGFS messages can hang the hub (in the fuse module.)

Platform: Linux

Subsystem: Global File System/Shell Backend

Symptom: When ten or more file system requests are outstanding, the fuse module and the hub lock up.

Resolution: Fixed

ISM Tool

Bug ID: 151734

Description: Possible ISM runtime migration bug.

Platform: Independent

Subsystem: ISM tool

Symptom: Converting ISMs as instructed in the Upgrade Tech Note results in an error:

```
/opt/opsware/twist/migration# ./ismrt-migrate.sh
[Info]***** The following ISM policies contain 2.x runtime file.
*****
[Info]/ (FolderRef:0)/Applications (FolderRef:1230001)/Solaris
Patching
(FolderRef:1530001)/Sun Patch Mgr 2.0
(SoftwarePolicyRef:1240001)
ISM applications containing old runtime files will be modified
to use the
latest runtime. Continue? (yes/no) yes
[Error]Failed to replace ISM runtime for policy: Sun Patch Mgr
2.0
Cause: No fields were updated in the input provided.
```

Resolution: Fixed

Jobs and Sessions

Bug ID: 160079/158959/160445

Description: Remediate with Preview Job does not show up in the NGUI job logs.

Platform: Independent

Subsystem: Jobs and Sessions

Symptom: Certain jobs are not logged in the NGUI job logs.

Resolution: Fixed

Model Repository

Bug ID: 153263

Description: Baseline upgrade fails when upgrading from SAS5.5.3 - 6.5.1.

Platform: Independent

Subsystem: Model Repository

Symptom: Core was uses a custom Oracle10g Enterprise Edition RPMS.

Data is exported from SAS 5.5.3 core into the 10g database.

While running the 6.5.1 upgrade script, the baseline data phase fails with errors:

```
ERROR: ORA-01400: cannot insert NULL into ("AAA"."ACTION_
ROLE"."ROLE_ID")
```

Resolution: Fixed

NAS/SAS Integration

Bug ID: 151466

Description: The Duplex match/mismatch icon not displayed.

Platform: Independent

Subsystem: NAS/SAS/ Integration – Duplex Compliance

Symptom: In NAS/SAS integration configuration, if Duplex is matched between a switch and a managed server interface, you should see:

- a green icon displayed on the Dashboard for the managed server.
- a green icon displayed for the managed server's Duplex in Compliance report.

If the Duplex is mismatched between a switch and a managed server interface, you should see:

- a red cross icon displayed on the Dashboard for the managed server.
- a red cross icon displayed for the managed server's Duplex in Compliance report.

These icons do not display. This was found to be a permissions problem.

Resolution: Fixed

Opsware Command Center (OCC)

Bug ID: 158736

Description: Unable to add device groups to user group if device group has same short name.

Platform: Independent

Subsystem: OCC Web

Symptom: You create three device groups:

```
3310001 'Device Groups/Public/Permissions Test/CCCCCCCCCCCC/Wholesale'
3290001 'Device Groups/Public/Permissions Test/BBBBBBBBBBB/Wholesale'
3280001 'Device Groups/Public/Permissions Test/AAAAAAAAAA/Wholesale'
```

All have the same short name of `Wholesale`.

Scenario 1: Add Device `Groups/Public/Permissions Test/AAAAAAAAAA/Wholesale` to the user group Advanced Users. The list refreshes properly.

Scenario 2: Add Device `Groups/Public/Permissions Test/BBBBBBBBBBB/Wholesale` to the user group Advanced Users. The list shows (2) attached device groups, but they are now both labeled

`Device Groups/Public/Permissions Test/BBBBBBBBBBB/Wholesale`

In addition, the Read and Read/Write radio buttons have disappeared for one of the device groups.

Scenario 3: Remove `Device Groups/Public/Permissions Test/BBBBBBBBBBB/Wholesale`. Both are removed from the list.

Resolution: Fixed

Bug ID: 155892

Description: OCC Client launcher doesn't work with a proxy server.

Platform: Independent

Subsystem: OCC Client

Symptom: When a user attempts to access the network through a Proxy, the launcher fails to connect to the core and returns a 'Cannot connect' error.

Resolution: Fixed

Bug ID: 158769

Description: Certain symlinks on managed servers can cause unexpected results from the NGUI.

Platform: Independent

Subsystem: OCC Client

Symptom: Create a symlink on a managed server similar to this:

```
mkdir -p /tmp/foo/bar
touch /tmp/foo/bar/foobar
mkdir -p /tmp/hello/world
cd /tmp/hello/world
ln -s ../../../../../../../tmp/foo/bar/foobar
```

When you attempt to use the NGUI to browse and view the contents of:

```
/tmp/hello/world/foobar
```

the NGUI becomes very busy and becomes unresponsive.

Resolution: Fixed

Opsware Installer

Bug ID:158483

Description: `mm_wordbot` doesn't have the correct location of `replicator.conf`.

Subsystem: Patch Management

Platform: Independent

Symptom: The Software Repository looks for the `replicator.conf` file under `/var/opt/opsware/word/etc/`.

`/etc/opt/opsware/replicator/*` is updated correctly, but `/var/opt/opsware/word/etc/` is not.

This is fixed in Opsware SAS 6.6. Earlier 6.x Opsware installations should create a symlink from

`/var/opt/opsware/word/etc/replicator.conf`

to

`/etc/opt/opsware/replicator/replicator.conf`

Resolution: Fixed

Bug ID: 152565

Description: The Opsware Installer fails when certain Opsware directories are symlinks (such as `/opt/opsware`)

Subsystem: Opsware Installer

Platform: Independent

Symptom: When performing a patch, if certain Opsware directories are a symlink (such as `/opt/opsware`), the patch will fail.

Resolution: Fixed

OS Provisioning

Bug ID: 155791/155822

Description: Solaris 10 exit codes not handled correctly

Platform: Solaris 10

Subsystem: OS Provisioning

Symptom: Use a 6.5.1 core to provision Solaris 10 x86 managed servers using Solaris Zones. When running an OS Sequence, the post-remediate steps are skipped because the Solaris "exit code 8" codes are treated as an error. Exit code 8 occurs when trying to install a patch for which the package doesn't exist.

Resolution: Fixed

Bug ID: 158071

Description: Prepare Solaris x86 OS on a Solaris Core - no packages are displayed.

Subsystem: OS Provisioning – Backend

Platform: Solaris

Symptom: 1: Import Solaris 10 x86 media to a Solaris 10 core.

2: Run Prepare OS.

Results:

- The OS Profile is created successfully
- No packages are displayed under the Packages tab

Resolution: Can't Reproduce

Bug ID: 158289

Description: Suse and Import Media Issue – several packages are not imported.

Subsystem: OS Provisioning Backend

Platform: Suse Linux

Symptom: After importing the Suse media, creating an OS Profile, adding packages to the OS Profile, then running the OS Sequence against a managed server, certain packages were not installed.

Resolution: Fixed

Bug ID: 158636

Description: Can't reprovision a device that lives in a non-core datacenter.

Subsystem: OS Provisioning Backend

Platform: Independent

Symptom: If a target device is located in a non-core datacenter Opsware SAS is unable to locate a build manager for reprovisioning. The re-provisioning job fails with an error logged in the session.

Resolution: Fixed

Bug ID: 158737/158636

Description: Can't re-provision an existing managed Solaris server.

Subsystem: OS Provisioning Backend

Platform: Solaris

Symptom: While attempting to re-provision a managed Solaris server the following error occurs:

```
Legacy Error Code: wayscripts.provisionOSerror Summary An
unidentified error occurred during provisionOS. Detail: An
unidentified error occurred during provisionOS. Resolution
Steps: View detailed output for more information regarding the
error. msg= No OS Build Manager in datacenter
```

Resolution: Fixed

Bug ID: 159127

Description: DOS Provisioning of HP DL585G2 needs additional device ID entry in `/etc/nics.map`.

Subsystem: OS Provisioning

Platform: Independent

Symptom: The dospopsw7.1 image provided by 6.5.x has the proper driver, but required one extra device ID to be added to the `/etc/nics.map`.

Original:

```
; From .\content\drivers\ndis\bxnd20x.cab
ret="BXND20X"
ven=14E4 "Broadcom"
dev=164c "Broadcom NetXtreme II Ethernet"
```

Modified:

```
; From .\content\drivers\ndis\bxnd20x.cab
ret="BXND20X"
ven=14E4 "Broadcom"
dev=164c "Broadcom NetXtreme II Ethernet"
dev=164a "Broadcom NetXtreme II Ethernet"
```

Resolution: Fixed

Bug ID: 159307

Description: Can't upload Red Hat EL 5 or Suse Linux ES-10 OS profiles in 6.5.1.4.

Subsystem: OS Provisioning – Backend

Platform: Red Hat/Suse Linux

Symptom: In Opsware SAS 6.5.1.4, `import_media` fails when importing Red Hat EL 5 or Suse Linux ES 10 media. The Web Services Data Access Engine also returns an exception if you try to upload an OS profile for Red Hat EL 5 or Suse Linux ES 10.

Resolution: Fixed

Bug ID: 160042

Description: Choose Customer as a part of Deploying OS Sequence.

Subsystem: OS Provisioning Backend

Platform: Independent

Symptom: The OS Sequence is too inflexible to decisions made at provisioning time. Someone who is deploying a sequence should be able to define the customer entity at deployment time. Currently, you must go to a separate screen to configure the Customer and attache it to the sequence. You can now define a customer using the Run OS Sequence wizard.

Resolution: Fixed

Patch Management

Bug ID: 150665

Description: It takes 35 seconds to get to report screen.

Subsystem: Patch Management

Platform: Independent

Symptom: Reports take a long time to generate. For example, using the NGUI, navigate to **Reports ➤ Compliance Reports ➤ Non-Compliant Patches By Server** or **Non-Compliant Patches By Patch Policy** report screen. It takes about 35 seconds to open the screen.

Resolution: Fixed

Bug ID: 152810

Description: SQL Server patches are not showing up in the Patch Library after MBSA patch database import.

Subsystem: Patch Management Windows – Backend

Platform: Windows

Symptom: Microsoft SQL Server patches are not showing up in the patch library after MBSA database import.

Resolution: Fixed

Bug ID: 153862

Description: Server compliance icons not auto updated.

Platform: Windows

Subsystem: Patch Management – Windows UI

Symptom: After a Compliance scan, the compliance dialog shows the status as completed, but the Compliance icon in the All Managed Servers list still displays the Scanning icon.

Resolution: Fixed

Red Hat Network Import

Bug ID: 159173

Description: `rhn_import` failed with `RHNetworkError: RHN Error: ProtocolError: <ProtocolError for rhn.redhat.com/rpc/api/: 404 Not Found>`

Platform: Red Hat Linux

Subsystem: Red Hat Network Import

Symptom: `rhn_import` fails with the error shown below. it appears that there is no retry when the error occurred. the script simply exits.

```
Nov 10 13:43:09 INFO [21331]: Importing 2853 of 2858: zlib-
1.2.3-3.i386
Nov 10 13:43:09 DEBUG [21331]: Found package in cache
Nov 10 13:43:18 DEBUG [21331]: Keeping package in download cache
Nov 10 13:43:18 INFO [21331]: Importing 2854 of 2858: zlib-
1.2.3-3.x86_64
Nov 10 13:43:18 DEBUG [21331]: Retrieving package details from
RHN
Nov 10 13:43:18 DEBUG [21331]: Traceback (most recent call
last):
  File "./bin/rhn_import_versioned.py", line 3191, in main
  File "./bin/rhn_import_versioned.py", line 2971, in doit
  File "./bin/rhn_import_versioned.py", line 3006, in do_channel
  File "./bin/rhn_import_versioned.py", line 3110, in import_
packages
  File "./bin/rhn_import_versioned.py", line 2281, in do_import
```



```
  File "./bin/rhn_import_versioned.py", line 2269, in get_
details
  File "./bin/rhn_import_versioned.py", line 2053, in get_
package_details
  File "./bin/rhn_import_versioned.py", line 1550, in __call__
  File "./bin/rhn_import_versioned.py", line 1532, in _method_
handler
RHNetworkError: RHN Error: ProtocolError: <ProtocolError for
rhn.redhat.com/rpc/api/: 404 Not Found>
Nov 10 13:43:18 ERROR [21331]: RHN Error: ProtocolError:
<ProtocolError for
rhn.redhat.com/rpc/api/: 404 Not Found>
```

Resolution: Fixed

Server Management

Bug ID: 155210

Description: Reboot server feature should have granular permissions control.

Platform: Independent

Subsystem: Server Management – Managed Servers

Symptom: The Server Reboot feature must be uniquely enabled via AAA rather than being automatically assigned as a by-product of a patch or software deployment.

This bug relates only to the UI action to reboot a server - it does not change how remediate functions because such reboot behavior is typically required for successful patch/software deployment.

Resolution: Fixed

Bug ID: 157788

Description: Can't see newly created servers in a dynamic group without pressing F5.

Platform: Independent

Subsystem: Server Management – Managed Servers

Symptom: In NGUI, create a new public dynamic server group. Then click on **Public**, then select the newly created dynamic group. Server names in this group should be displayed.

However, the server names are not displayed. You must press F5 (Refresh) to get the server names to display inside dynamic server group.

Resolution: Fixed

Software Management

Bug ID: 148797

Description: Compliance status is not updated after remediation if the server is in different core in a mesh.

Platform: Independent

Subsystem: Software Management API - Compliance

Symptom: A Managed Server is in a Slave core. A user logs in to the Master Core and runs a remediation job.

1. Login to the Master Core.

2. Attach a policy containing a package to a server.

3. Run a software compliance scan – the server status correctly becomes non compliant.

4. Remediate the server

The job completes, but the compliance status for the server does not change to compliant – it still shows as non compliant.

Resolution: Fixed

Bug ID: 151292

Description: A software package is not unlocked after a complete migration.

Platform: Independent

Subsystem: Software management Tools - Migration

Symptom: Upload a package and assign customer. Add the package to an application node. Then start a full migration and complete it.

After the complete migration, the package should be unlocked, but is not. It should be unlocked during the migration process.

Resolution: Fixed

Bug ID: 154951

Description: RPM install order does not honor dependencies.

Platform: Independent

Subsystem: Software Management Backend – Remediate (RPM Packages)

Symptom: When multiple RPMs can satisfy a dependency and there are non-RPMs interleaved, the RPMs are added to the end of the install list instead of being placed before the dependency they satisfy.

Resolution: Fixed

Bug ID: 157030/157434/158315

Description: `NOT_ADOPTABLE` package logic is too restrictive.

Platform: Independent

Subsystem: Software Management Backend – Remediate (RPM Packages)

Symptom: When remediating a system, if a package is already installed it is *adopted*. Some package types, however, (Solaris Patches in particular) are listed as *not adoptable* and we don't differentiate between managed or unmanaged packages when we choose not to adopt a particular package at remediate time. Even if a package is marked *not adoptable*, it should be checked to see if it is managed, and if so, adopt it. and, if so, adopt it.

Resolution: Fixed

Bug ID: 157712

Description: Software Policy remediate stalls at step 1 when unreachable servers and device groups are in server usage.

Platform: Independent

Subsystem: Software Management – Software Policy

Symptom:

1. Create a device group and add unreachable servers to it.
2. Add to a software policy from Server Usage the device group you have created as well as few reachable and unreachable servers.
3. Select all servers and the device group from Server Usage, right click, remediate.

The screen will stall on step 1 (Server and Policies) with message Loading.

Resolution: Can't Reproduce

Bug ID: 158822

Description: RPM Compliance calculations fail when there are non-numeric characters in version or release strings.

Platform: Independent

Subsystem: Software Management - Compliance

Symptom: Packages with a non-numeric string (such as, `EL`) cause RPM compliance calculations to fail. No detailed compliance information is generated in the database and consequently reports do not provide any meaningful information.

Resolution: Fixed

Bug ID: 159583/160055

Description: NGUI calls `getResult` multiple times when viewing a completed job.

Platform: Independent

Subsystem: Software Management UI - Install/Uninstall/Remediate

Symptom: You have several large Install Software Template. When you attempt to view them the Web Services Data Access engine runs out of memory and fails.

Resolution: Fixed

Bug ID: 160084

Description: Four policies attached to a server, contents for only three of the policies installed.

Platform: Independent

Subsystem: Software Management – Other

Symptom: Four storage policies added to a Solaris 9 managed server, only the packages for Three of the policies were installed on the server.

For example:

1: Assimilate Solaris 9 server to newly created SAS + ASAS core.

2: Attach following software policies:

- Storage Agent for Brocade
- Storage Agent for HiCommand
- Storage Agent for McDATA.
- Storage Agent for NetApp.

3: Remediate the policies.

4: View Job Status results and attached policies.

Actual Results:

The Job status only shows the contents for the first three policies as having been downloaded and installed on the server. The contents for NetApp were not deployed or installed even though the NetApp policy is associated with the server.

Resolution: Fixed

Bug ID: 160757

Description: Ticket ID is not accessible on "Run ISM Control" jobs.

Platform: Independent

Subsystem: Software Management UI – Run ISM Controls

Symptom: A user submits a **Run ISM control** job from the NGUI. In the job wizard, the user enters a Change Ticket ID to allow Approval integration. The Ticket ID is not visible in the Job Log history. Since the Ticket ID is used for PAS Approval integration, this missing field impacts ISM controls.

Resolution: Fixed

Bug ID: 160940

Description: yum multi-arch issue on x86_64

Platform: Red Hat EL x86_64

Subsystem: Software Management Backend – Remediate (RPM Packages)

Symptom: A Red Hat x86_64 machine has `cracklib.x86_64` and `cracklib-dicts.x86_64` installed. Attempting to install `cracklib.i386` fails. Although this is an issue in yum, not SAS itself.

Resolution: Fixed

Software Repository

Bug ID:160625

Description: `mm_wordbot.args rpms_not_upgradable` configuration option needs to be updated.

Platform: Linux

Subsystem: Software Repository

Symptom: The `rpms_not_upgradable` configuration option needs the following packages added:

- `kernel-smp-devel`
- `kernel-hugemem-devel`
- `kernel-largesmp-devel`

In addition, SAS should check RPMs against this configuration file to see if the uploaded RPM *provides* any of the entries in the list (currently SAS only checks the name of the uploaded RPM against the list, but ignores the entries that the RPM provides).

Resolution: Fixed

Virtualization

Bug ID: 157157/157154/157358

Description: Virtualization UI could be more efficient, many calls to the Web Service Data Access Engine made.

Platform: Independent

Subsystem: Virtualization UI

Symptom: Launch the NGUI. Before the server cache finishes updating, click on Virtual Servers

This creates a listener which listens for server cache updates (add/update/remove) and for each of these events launches a new thread to reload the entire virtual server list. Since this load takes a long time, there could be thousands of threads launched. Other performance issues.

Resolution: Fixed

Bug ID: 160839/161304

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 is created, select Servers ‰ Virtual Servers. The newly created VM is shown as an unmanaged VM. Its Hostname is blank, and its Virtual Machine Name is that of the host ESX 3 server.

Resolution: Fixed

Bug ID: 160925

Description: scan of ESX 3 server fails with
`AuthorizationDeniedException: <Access denied>`
`<operation=DefaultOperations.updateHypervisorInventory>`

Platform: Independent

Subsystem: Virtualization Backend (VMWare)

Symptom: In certain situations an `appConfig push` can cause a corrupted thread and subsequently, when a virtualization scan is done, the corrupted thread causes update authorization to fail.

Resolution: Fixed

Bug ID: 161394/161452

Description: NSCD error when trying to create a solaris zone for solaris 10 U4 / Solaris zone creation reports **Succeeded** but the zone is not reachable.

Platform: Solaris

Subsystem: Virtualization – Backend (Zones)

Symptom: You create a zone under Solaris and assign it an IP address. The job finishes successfully, however, the zone is not reachable on the assigned IP address. Although the zone is created and is running on the hypervisor machine, the zone's network is not correctly configured (the netmask is incorrect).

Resolution: Fixed

Chapter 5: Known Problems, Restrictions, and Workarounds in Opsware SAS 6.6

IN THIS CHAPTER

This chapter describes workarounds for known problems in Opsware SAS 6.6. These descriptions are arranged by the following features:

- Application Configuration
- Audit and Remediation
- Code Deployment and Rollback
- DCML Exchange Tool (DET)
- Global Filesystem/Shell
- NAS/SAS Integration
- Operating System Provisioning
- Opsware Agent
- Opsware Installer
- Opsware SAS Client
- Opsware SAS Web Client
- Patch Management for Windows
- Patch Management for Unix
- Remediation
- SAS Client Reports
- Software Management
- Virtualization
- Visual Application Manager (VAM)
- Visual Packager

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

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:

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

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

ouplоad  -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.

Code Deployment and Rollback

Bug ID: 145470

Description: Code Deployment and Rollback (CDR) Not Supported on an VMware ESX Hypervisor.

Platform: VMWare ESX 3

Subsystem: Code Deployment and Rollback

Symptom: If you attempt to use the Code Deployment and Rollback features on a VMWare ESX 3 hypervisor, it will not work. This feature is not supported on VMware ESX hypervisor servers.

Workaround: Configure the ESX firewall to allow connections between the source and target computers at TCP port 1002.

DCML Exchange Tool (DET)

Bug ID: 130600

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

Platform: Independent

Subsystem: DET Import

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

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

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

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.

Workaround: Check the RDF file to verify that multiple files were exported.

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: 129501

Description: Changing the encoding with the `swenc` command might cause problems for background processes.

Subsystem: SAS Client - Global Shell

Platform: Linux

Symptom: In a Global Shell session, change the encoding with the swenc command. Background processes that are running in the Global Shell session might fail.

Workaround: Wait until background processes have completed before changing the encoding with `swenc`.

Bug ID: 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

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: 141568

Description: Within an Opsware Global Shell session, `scp` to a remote server does not work.

Platform: Independent

Subsystem: Global Shell

Symptom: The `scp` command fails with the following error message: `No such file or directory lost connection`.

Workaround: To copy a file from the OGFS to a non-managed server, run `scp` on the non-managed server. To copy a file from the OGFS to a managed server, use the `cp` command within the Global Shell and copy the file to `/opsw/Server/@/<server>/files/<login>/<target-path>`.

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`).

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.

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.

Opsware Agent

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: 134679

Description: The Opsware Discovery and Agent Deployment feature is unable to deploy agents to Windows servers if the system's Local Security Policy is set to the default by certain releases of Windows XP.

Subsystem: ODAD

Platform: Windows

Symptom: Some releases of Windows XP set the Local Security Policy to a default that does not permit agent deployment. If the Local Security Option "Network Access: Sharing and security model for local accounts" is set to the value "Guest only - local users authenticate as Guest" then all attempts to deploy Opsware Agents using ODAD will fail with an incorrect user name or password error.

Workaround: Perform the following steps to change the option:

1. Log in to the unmanaged server using remote desktop.

2. Navigate to **Control Panel ➤ Administrative Tools ➤ Local Security Policy**.
3. Select **Local Policies ➤ Security Options**.
4. Scroll down to the option “Network access: Sharing and Security Model for local accounts” and then double click to select it.
5. Change the default to “Classic - local users authenticate as themselves”.
6. Click **Apply** then click **OK**.

Opsware 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.

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: 149059

Description: If the server hosting the Software Repository is marked unreachable when you try to upload the Opsware SAS content component, the upload process fails.

Subsystem: Opsware Software Repository

Platform: Independent

Symptom: You tried to upload the Opsware SAS content component when the Software Repository server was marked unreachable. The upload failed with a `wordbot.accessDenied` error.

Workaround: Run the server communications test to verify whether the Software Repository server is marked unreachable. See "Searching for Unreachable Servers" in the *Opsware® SAS User's Guide: Server Automation*.

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: 149346

Description: The Opsware Installer does not return an appropriate error message when the action file is invalid.

Subsystem: Opsware Installer

Platform: Independent

Symptom: You ran the Opsware Installer with an invalid action file and it returned the following error message:

```
Opsware Installer has encountered an error:
Error Type: exceptions.KeyError
Error Value: components
Exiting Opsware Installer.
```

Workaround: There is a possible error in the action file you are trying to use. Check the action file, correct any errors in syntax, and re-run the Opsware Installer.

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.

Opsware 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.

Gateway Installation

Bug ID: 146262

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

Platform: Any

Subsystem: Installation

Symptom: The load balancer Gateway starts without a problem, but there is no logging directory (`/var/log/opsware/opswgw-lb`) and, hence, no logs.

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

Opsware 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.

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

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

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 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 multibyte character. Multibyte 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.

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 6.6.

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 6.6.

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

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

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 Opware 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.

Chapter 7: Contacting Opsware, Inc.

IN THIS CHAPTER

This chapter contains the contact information for Opsware Technical Support and Opsware Training:

- Opsware Technical Support
- Opsware Training

Opsware Technical Support

To contact Opsware Technical Support:

Phone: +1 877 677-9273 (1-877-Opsware)

E-mail: support@opsware.com

For information about Opsware Technical Support:

URL: https://download.opsware.com

Opsware Training

To contact Opsware Training:

E-mail: education@opsware.com

Opsware, Inc. offers several training courses for Opsware users and administrators.

For information about Opsware Training:

URL: www.opsware.com/education

