Opsware® SAS 6.5 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 6.5

IN THIS CHAPTER

This chapter contains the following topics:

Opsware Server Automation System (SAS) 6.5 provides a core set of features that automate critical areas of server and application operations – including the provisioning, deployment, patching, and change management of servers – across major operating systems and a wide range of software infrastructure and application products.

Opsware SAS 6.5 also provides several new features and performance enhancements:

- Opsware Launcher
- Audit and Remediation New Features and Enhancements
- IIS Metabase and COM+ Support in Visual Packager
- Application Configuration Ordering Maintained in Software Policies
- Job Approval Integration
- Opsware Operational Management Database (OMDB)

Opsware Launcher

The SAS Client Launcher is a self-contained Java application that allows you to access the SAS Client from any core in your mesh. You can install the SAS Client Launcher without needing administrator privileges, and once installed, it will not interfere with or depend upon any other version of Java Web Start you may have installed on your system.

You can use the Launcher to log in to and download the latest version SAS Client. If the SAS Client has been upgraded on a specific core or on a core in a different mesh, you can choose which core you would like to use for downloading the SAS Client. The SAS Client Launcher also allows you to configure advanced settings, such as debug settings, locale settings, and access to the Java Web Start that runs the Launcher and SAS Client.

Audit and Remediation New Features and Enhancements

The following Audit and Remediation features are new in the 6.5 Release:

- Audit Rule Exceptions
- New TON Audit and Remediation Content
- Full Remediation for COM+ Objects
- Remediation of Microsoft IIS Metabase Objects

Audit Rule Exceptions

Audit Rule Exceptions allow you to create temporary or permanent rule exceptions on servers (or groups of servers) in audit, allowing you to exclude specific rules on selected target servers of the audit when the audit runs. You can set an expiration date for rule exceptions to make sure that when the exception is no longer needed or permitted, the rule will once again be applied to all servers in the audit. You can also add a written explanation for the exception and associate a ticket ID with it.

New TON Audit and Remediation Content

Audit and Remediation for SAS 6.5 also includes new Audit Policies for The Opsware Network (TON) subscribers. If you subscribe to TON, you can be kept up to date on the latest industry compliance standards based on the needs of your data center. For information about subscribing to TON, see your Opsware sales representative.

Full Remediation for COM+ Objects

With the new "archive all associated contents" option for Audit and Remediation COM+ Rules, you can now fully remediate servers that do not comply with the compliance standards defined in your audits and snapshots. All you need to do is select the "archive all associated contents" option when you configure a COM+ rule in an audit or snapshot, and you can remediate any servers that so not meet the rule definition.

Remediation of Microsoft IIS Metabase Objects

You can now perform remediation of Microsoft IIS Metabase objects.

IIS Metabase and COM+ Support in Visual Packager

You can now create packages using Visual Packager that include Microsoft IIS Metabase and COM+ objects.

Application Configuration Ordering Maintained in Software Policies

In this release, application configuration order is maintained across multiple child software policies contained within a parent software policy. For each child software policy containing application configurations, those application configurations are applied immediately following the policy's packages and before the next child policy's packages are installed.

Job Approval Integration

Opsware SAS jobs perform operations such as remediating policies, installing patches, and running OS sequences. In many IT environments, such operations must be approved and assigned tickets before they can execute. This release of Opsware SAS enables the integration of Opsware SAS jobs with ticketing and approval systems such as BMC Remedy Help Desk. To implement this new feature, Opsware SAS ships with a connector that contacts the Opsware Process Automation System (PAS) and then runs an Ops flow on the PAS server. An Ops flow can coordinate the job approval workflow by making calls to both BMC Remedy Help Desk and Opsware SAS.

For example, a job launched by the SAS Client can block, pending approval by BMC Remedy Help Desk. Behind the scenes, an Ops flow can create a Remedy Action Request (AR) ticket, update the SAS job with the ticket ID, and change the status of the SAS job.

For instructions on enabling job approval and configuring the PAS connector, see the Opsware Automation Platform Developer's Guide.

Opsware Operational Management Database (OMDB)

Opsware Operational Management Database (OMDB) is a configuration management database designed to create and maintain a record of the infrastructure data in your IT environment. It has the ability to store information from Opsware SAS, Opsware NAS, and as well as other third party systems. You can use the OMDB Search, Reports, and Dashboard features to view and analyze IT infrastructure such as applications, servers, networks, and storage.

For more information about the OMDB, see the OMDB 1.0.1 Release Notes.

Chapter 2: Platform and Environmental Support

IN THIS CHAPTER

This chapter contains the following topics:

- Supported Operating Systems
- Supported Core Operating Systems
- Operating System Deprecation and End of Support
- Supported Installations and Upgrades for Opsware SAS 6.5
- Documentation for Opsware SAS 6.5

Supported Operating Systems

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

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)	PA-RISC PA-RISC PA-RISC PA-RISC and Itanium

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

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
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 Solaris 10	Fujitsu SPARC 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
Red Hat Linux	Red Hat Linux 7.3 Red Hat Linux 8.0 Red Hat Enterprise Linux 2.1 AS Red Hat Enterprise Linux 2.1 ES Red Hat Enterprise Linux 2.1 WS Red Hat Enterprise Linux 3 AS Red Hat Enterprise Linux 3 ES Red Hat Enterprise Linux 3 WS Red Hat Enterprise Linux 4 AS Red Hat Enterprise Linux 4 ES Red Hat Enterprise Linux 4WS Red Hat Enterprise Linux Server 5 Red Hat Enterprise Linux Desktop 5	32 bit x86 32 bit x86 32 bit x86 32 bit x86 32 bit x86 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86

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

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
SUSE Linux	SUSE Linux Enterprise Server 8 SUSE Linux Standard Server 8 SUSE Linux Enterprise Server 9 SUSE Linux Enterprise Server 10	32 bit x86 32 bit x86 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86
VMware	ESX Server 3	32 bit x86 and 64 bit x86

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

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 Windows XP Windows 2003 Windows 2000	32 bit x86 and 64 bit x86 32 bit x86 32 bit x86 32 bit x86

Supported Core Operating Systems

This section 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*.

The following table lists the supported operating systems for the Opsware core components.

Table 2-3: Opsware Core Supported Operating Systems

SUPPORTED OS FOR OPSWARE CORE	VERSIONS	ARCHITECTURE	OPSWARE COMPONENTS
Sun Solaris	Solaris 8	Sun SPARC	All components, *excluding* the Opsware Global File System Server (OGFS) component
Sun Solaris	Solaris 9	Sun SPARC	All components
Sun Solaris	Solaris 10	Sun SPARC, Niagara	All components
Red Hat Linux	Red Hat Enterprise Linux 4 AS	64 bit x86	All components
Red Hat Linux	Red Hat Enterprise Linux 3 AS	32 bit x86	All components

The following table lists the supported operating systems for the following components of an Opsware Satellite:

- 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

Table 2-4: Opsware Satellite Supported Operating Systems

SUPPORTED OS FOR OPSWARE SATELLITE	VERSIONS	ARCHITECTURE
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 6.5:

- 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 6.5:

- 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 6.5

The Opsware SAS 6.5 release supports the following installations:

- New installations of a standalone core
- New installations of a multimaster mesh
- New installations of a Satellite
- Upgrading a standalone core from Opsware SAS 5.3, 5.5.1, 5.5.2, or 5.5.3 to 6.5
- Upgrading a multimaster mesh from Opsware SAS 5.3, 5.5.1, 5.5.2, or 5.5.3 to 6.5
- Upgrading an Opsware Satellite from Opsware SAS 5.3, 5.5.1, 5.5.2, or 5.5.3 to 6.5
- Upgrading a standalone core from Opsware SAS 6.0.1, 6.0.2, 6.1, 6.1.1, or 6.1.2 to 6.5
- Upgrading a multimaster mesh from Opsware SAS 6.0.1, 6.0.2, 6.1, 6.1.1, or 6.1.2 to 6.5
- Upgrading an Opsware Satellite from Opsware SAS 6.0.1, 6.0.2, 6.1, 6.1.1, or 6.1.2 to 6.5

Documentation for Opsware SAS 6.5

This release comes with the following documentation:

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

The Opsware SAS documentation is available online at

https://download.opsware.com/kb/category.jspa?categoryID=20

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

Chapter 3: Opsware Agent Compatibility

IN THIS CHAPTER

This chapter contains the following topic:

- Opsware Agent Compatibility

Opsware Agent Compatibility

The majority of the Opsware SAS Web Client features for Opsware SAS 6.5 are compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 6.5 features with Opsware Agent versions prior to 6.5 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: Important Fixes in Opsware SAS 6.5

IN THIS CHAPTER

This chapter contains bugs that have a severity level of Critical or Major and are fixed in Opsware SAS 6.5. These descriptions are arranged by the following features:

- Global Shell
- Intelligent Software Module (ISM) Development Kit
- Opsware API
- Opsware Installer
- SAS Client
- OS Provisioning
- Reports
- Software Management
- Visual Application Manager (VAM)

Global Shell

Bug ID: 132935

Description: Global Shell audit directory has read-any access.

Subsystem: SAS Client - Global Shell

Platform: Independent

Symptom: The Global Shell audit directory could be read by any Unix user with a login to the core server. It could also be read from within a Global Shell session if the user had file system permissions to the core server.

Resolution: Fixed.

Bug ID: 146106

Description: Upgrade slow for Global Shell audit file system that is NFS mounted.

Platform: Independent

Subsystem: Global Shell Backend

Resolution: Fixed.

Intelligent Software Module (ISM) Development Kit

Bug ID: 135455

Description: Some ISMs force files to be installed in "C:\Program Files" on 64-bit Windows systems.

Platform: 64-bit Windows

Subsystem: ISM

Summary: This problem affects ISMs (containing MSIs) created with ismtool or the Visual Packager. When such a packages is created on a 64-bit Windows server, "C:\Program Files" is hardcoded into the paths of some of the files within the package, even if the files do not reside in "C:\Program Files." Later, when the ISM is installed on a managed server, the files are placed in "C:\Program Files."

Resolution: Fixed

Opsware API

Bug ID: 143592

Description: The getPlatformVOs method throws NotFoundException.

Platform: Independent

Subsystem: Opsware API

Symptom: If the parameter passed to the getPlatformVOs method includes non-existent platform refs, the method throws NotFoundException, but it should just filter out the non-existent platforms from the returned list.

Resolution: Fixed

Bug ID: 145371

Description: Search attribute names are wrong for AuditResult and SnapshotResult objects.

Platform: Independent

Subsystem: Opsware API

Symptom: Prior to Opsware SAS 6.5, the following incorrect search attributes were used:

```
SnapshotResultsVO.createdBy
SnapshotResultsVO.creatorType
SnapshotResultsVO.createDate
SnapshotResultsVO.pK
SnapshotResultsVO.name
AuditResultsVO.createdBy
AuditResultsVO.createdDate
AuditResultsVO.pK
AuditResultsVO.name
AuditResultsVO.nonCompliantObjectCount
AuditResultsVO.policyPlatformType
```

In 6.5 the search attribute names were corrected as shown in the following list. Notice that the strings change from Results to Result.

```
SnapshotResultVO.createdBy
SnapshotResultVO.creatorType
SnapshotResultVO.createDate
SnapshotResultVO.pK
SnapshotResultVO.name
AuditResultVO.createdBy
AuditResultVO.createdDate
AuditResultVO.pK
AuditResultVO.name
AuditResultVO.nonCompliantObjectCount
AuditResultVO.policyPlatformType
```

If a saved search uses the old attribute names, the search must be modified to use the new names.

Resolution: Fixed

Opsware Installer

Bug ID: 137926

Description: The Opsware Global File System Server (OGFS) component did not start after installing an Opsware core.

Subsystem: Opsware Global File System Server (OGFS)

Platform: Independent

Symptom: In the Opsware SAS client, launching the Global Shell causes an authentication error and the shell will not function.

Resolution: Fixed.

Bug ID: 141553

Description: The Satellite Gateway installer fails if the Agent is installed and running.

Platform: Independent

Subsystem: Opsware Installer

Symptom: If you run the Satellite Installer and choose Gateway to install on a managed server, you will get an error message (similar to the following example) at the end of install script:

```
WARNING: an error was detected while running an external
command or script.  The output follows:
Verifying dependencies
Verify "localhost" not listening on port 1002: FAILURE (Port
already
allocated).
[Nov-06-2006 08:19:46] Component installation script encountered
an error (exit
status 1)
[Nov-06-2006 08:19:46] Exiting Opsware Installer.
```

With this failed installation, the new realm does not appear in the drop-down list in the ADT interface (“Unmanaged Servers”).

For more details, see the file that resembles the following path:

```
/var/log/opsware/install_opsware/install_opsware.2006-11-
06.08:14:24_verbose.log
```

When the script is done, the file resembles the following path:


```
/var/log/opsware/install_opsware/install_opsware.2006-11-
06.08:14:24.log
```

Resolution: Modified the Opsware Installer so that it verifies that no Agent is installed on a Satellite server prior to beginning the installation process.

Bug ID: 141965

Description: The Data Access Engine (twist) stops ack'ing TIBCO messages and causes Ledger growth.

Platform: Independent

Subsystem: Opsware Installer

Symptom: The following message occurs on multimaster cores stating that a particular TIBCO client is not acknowledging TIBCO traffic:

```
2006-11-14 15:18:24 RV: TIB/Rendezvous Error Not Handled by
Process:
{ADV_CLASS="WARN" ADV_SOURCE="RVCM"
ADV_NAME="DELIVERY.NO_RESPONSE.130.177.110.81_1026"
listener="130.177.110.81_1026"}
```

Resolution: Fixed.

Bug ID: 144376

Description: Garbage collector can break multi-phase session chains.

Platform: Independent

Subsystem: Opsware Model Repository

Symptom: Certain way tasks involve multiple phases where each phase is represented as a separate session. These sessions are linked together by the `prev_phase` session parameter. If the multi-phase session chain spans multiple days, the way session garbage collector can delete the older sessions in the chain leaving a `prev_phase` value that refers to a session that no longer exists.

Resolution: Fixed.

Bug ID: 145549

Description: The Installation Guide does not have specific Solaris 10 prerequisites.

Platform: Independent

Subsystem: Opsware Installer

Symptom: When installing Oracle on Solaris 10 the Opsware Installer does not explicitly check for the following prerequisite packages: `SUNWpool`, `SUNWpoolr` and `SUNWmfrun`.

Resolution: The *Opsware® SAS Planning and Installation Guide* has been updated and includes a list of the packages required for Solaris 10.

Resolution: Fixed.

Bug ID: 145621

Description: The Data Access Engine (twist) fails to start if the `DefaultAuthenticatorInit.ldif` file is not readable.

Platform: Independent

Subsystem: Opsware Installer

Symptom: During the installation process, the following error message appears:

```
A required file /var/opt/opsware/twist/
DefaultAuthenticatorInit.ldift is not readable.
Please ensure that the file is readable.
opsware-sas: "twist" failed to start
Failed to perform "start" operation on Opsware SAS
components.
```

Resolution: Fixed.

Bug ID: 147551

Description: The `unmodel_os_packages.sw.pyc` script has the wrong file permissions and owner.

Platform: Independent

Subsystem: Opsware Installer

Symptom: During an upgrade process, when you tried to run `/opt/opsware/spin/util/unmodel_os_packages.sw.pyc`, the following error occurred:


```
[root@indigo1 util]# /opt/opsware/spin/util/unmodel_os_
packages.sw.pyc --h
-bash: /opt/opsware/spin/util/unmodel_os_packages.sw.pyc:
Permission denied
```

Resolution: Fixed.

Bug ID: 148011

Description: Device group recalculation will hang due to conflicts.

Platform: Independent

Subsystem: Opsware Installer

Symptom: Conflicts were generated with the net result of recurring Data Access Engine (twist) log entry on all but two cores in the mesh, for the appropriate ID:

```
OpswareError: spin.multimasterConflict [ module: spinobj.py,
method: saveInner, line: 912, hostname: usahsow002,
timestamp: 11/Apr/2007 183157, msg:  Object
'_DataCenterConfigValue ID 10120102-0' is read-only until a
conflict is resolved ]
```

Resolution: Fixed.

Bug ID: 148987

Description: Simultaneous multi-request transactions cause Oracle errors.

Platform: Independent

Subsystem: Opsware Installer

Symptom: If many threads are all writing through the Spin to the same object at the same time, various Oracle errors can be thrown, including:

```
ORA-00000
ORA-20061
ORA-20064
```

Resolution: Fixed.

OS Provisioning

Bug ID: 139032

Description: OS Sequences Allowed Adding an OS Installation Profile that Did Not Match the OS Sequence

Platform: Any

Subsystem: OS Sequences and OS Profiles

Symptom: Previously, when you created an OS Sequence, the user interface would allow you to add an OS Installation Profile from an operating system different than the OS Sequence. When you saved the OS Sequence, it would be saved to the By Type location in the library based upon the OS Installation Profile, which could cause some users to believe their OS Sequence was not saved. In fact, the OS Sequence was saved, but to the folder based upon the operating system of the OS Sequence.

Resolution: This has been fixed. When you create an OS Sequence in SAS 6.5, you will only be able to view and add OS Installation Profiles that match the operating system of the OS Sequence. For OS Sequences that were created prior to SAS 6.5, you will still be able to view an OS Installation Profile from an operating that is different from the OS Sequence, but you will get a warning dialog if you attempt to add the non-matching OS Installation Profile.

Bug ID: 142005

Description: Previously could not upload new configuration files for OS Definitions/OS Installation Profiles with attached packages

Platform: Solaris/Linux

Subsystem: OS Provisioning - OS Definitions/OS Installation Profiles

Symptom: For Solaris or Linux OS Definitions/OS Installation Profiles that were created previous to the SAS 6.5 release and that contain attached packages, you were not able to upload a new configuration files to those OS Definitions/OS Installation Profiles.

Resolution: Fixed

Bug ID: 142102

Description: Partition on the front of the disk for Linux OS Provisioning not always large enough for RH4 kernel

Platform: Red Hat Linux RH4

Subsystem: Linux OS Provisioning

Symptom: Sometimes during the process of provisioning a bare metal server with Linux RH4, there have been problems with the temporary boot partition being unable to hold the Linux kernel due to a disk partitioning size issue. This would cause the provisioning to fail.

Resolution: Fixed

Bug ID: 149164

Description: Remediate Was Failing on Windows 2000 with no SPs Booted from WinPE During OS Provisioning

Platform: Windows 2000

Subsystem: OS Provisioning Remediation

Symptom: Remediation was hanging and would fail when provisioning a Windows 2000 server that had no service packs and that was booted from the WinPE pre-installation environment.

Resolution: Fixed

Bug ID: 149164

Description: Remediate Was Failing on Windows 2000 with no SPs Booted from WinPE During OS Provisioning

Platform: Windows 2000

Subsystem: OS Provisioning Remediation

Symptom: Remediation was hanging and would fail when provisioning a Windows 2000 server that had no service packs and that was booted from the WinPE pre-installation environment.

Resolution: Fixed

Reports

Bug ID: 136305

Description: Customer/Facility Permissions and Device Group Permission Overrides report taking long time to run and not all results viewable. SAS Client may hang.

Platform: Independent

Subsystem: SAS Reports - User and Security Reports

Resolution: Updated the http parameter to `proxy_no_filter`. Modified the code to export reports for SAS so that it uses the same code that the OMDB uses for HTML. The export for .xls or .html with SAS will use the HTML export code from the OMDB. The NGUI proxy uses the `com.opsware.ngui.webdatarelay.max_rows_allowed` system property to determine the maximum TR tags in report HTML, such as `com.opsware.ngui.webdatarelay.max_rows_allowed=1000`. To override the default value of `5000`, add your property override to the jnlp file.

SAS Client

Bug ID: 144896

Description: Creating a dynamic device group using advanced search did not list the members of the group immediately.

Subsystem: SAS Client - Device Groups

Platform: Independent

Resolution: Fixed

Software Management

Bug ID: 144841

Description: In the SAS Client, deleting a folder containing many packages caused the SAS Client to stop responding. After the folder was deleted the SAS Client would start to respond again.

Subsystem: SAS Client - Software Management

Platform: Independent

Resolution: Fixed.

Bug ID: 146000

Description: Uploading packages or patches after uploading a BCS script caused the Customer to be same as the BCS Customer.

Platform: Independent

Subsystem: SAS Client - Software Management

Resolution: Fixed.

Bug ID: 146394

Description: Attempting to install multiple architectures of the same RPM for a platform using software policy would fail.

Subsystem: SAS Client - RPM Deployment

Platform: Red Hat Linux

.**Resolution:** Fixed.

Visual Application Manager (VAM)

Bug ID: 139071

Description: For .vam files that resided on the hub, instead of opening the selected (older) topology, the SAS Client opened the most recent saved topology when you clicked **Open**.

Platform: Independent

Subsystem: SAS Client - Visual Application Manager

Symptom: You selected an older topology from a .vam file on the hub and clicked Open. The most recent topology was displayed, instead of the one that you selected.

Resolution: Fixed

Bug ID: 145823

Description: New Application Tier windows were missing Server Filter field (and title bar says “Edit Application”) when you created a new tier from the top level application node.

Platform: Independent

Subsystem: Visual Application Manager (VAM)

Symptom: If you selected the top level node in the Application tree inside VAM and created a new application tier, the title bar of the new application tier window would incorrectly say Edit Application Tier, and the window will not have a server filter.

Resolution: Fixed

Bug ID: 145933

Description: VAM and SAS Client would sometimes hang when scanning multiple servers through a Solaris 9 or Solaris 10 Opsware Global File System (OGFS) (hub).

Platform: Solaris 9 and Solaris 10

Subsystem: Visual Application Manager (VAM) - Opsware Global File System (OGFS)

Symptom: If a user ran a single VAM scan on multiple servers - typically more than 30 physical or virtual servers - and the Opsware Global File System (OGFS) was running on Solaris 9 or Solaris 10, in some cases the OGFS server process would hang for up to ten minutes and the scan would fail.

Workaround: Fixed

Chapter 5: Known Problems, Restrictions, and Workarounds in Opsware SAS 6.5

IN THIS CHAPTER

This chapter describes workarounds for known problems in Opsware SAS 6.5. These descriptions are arranged by the following features:

- Application Configuration
- Audit and Remediation
- DCML Exchange Tool (DET)
- Global Shell
- NAS Integration
- Operating System Provisioning
- Opsware Agent
- Opsware API
- Opsware Installer
- Opsware SAS Client
- Opsware SAS Web Client
- Patch Management for Windows
- Patch Management for Unix
- SAS Client Reports
- Software Management
- 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: 147566

Description: Application Configuration Cannot Be Pushed Before a Package in a Software Policy

Platform: Independent

Subsystem: Software Policy - Application Configuration Pushed After Package Install

Symptom: If you have a software policy that contains both an application configuration and a package, when you remediate the policy the package will be installed first, followed by the application configuration push. Currently, there is no means to change this installation order.

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.

Bug ID: 148219

Description: Cannot add and save rule exceptions to a pre-SAS 6.5 Audit unless the compliance migration Script has been run

Platform: Independent

Subsystem: Audit and Remediation - Content Migration

Symptom: If you are upgrading to SAS 6.5, and you have preexisting audits, if you attempt to add exceptions to those audits (a new Audit and Remediation feature in SAS 6.5), you will not be able to save the rule exceptions.

Workaround: Consult the Opsware SAS 6.5 Content Migration Guide for instructions on how to run the compliance migration script.

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: Here's an example scenario where this problem occurs:

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

In this scenario, the preview incorrectly shows that the app will be renamed because it is in use by a template. The actual import will correctly delete the app. This problem also occurs when other objects are detached and deleted, for example, app/package, app policy/app 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 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 Administrators group to browse 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 we ship with the product 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: User can edit their .bash_profile and change the PS1 setting to the following:

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

Bug ID: 133316

Description: On Solaris OGFS, rosh (ttlg) commands for Windows filesystems 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 if it's running on Linux. This problem occurs when a user in a Global Shell session cd's into a Windows filesystem directory and issues a rosh (ttlg) command that uses a different case than what appears in the OGFS. Although the names in a Windows filesystem are not case sensitive, the hub is hosted on a Unix server, which has Unix filesystem semantics with respect to case.

Here's an example that reproduces this problem:

```
$ 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: Users must observe filesystem case even when they cd into the filesystems of Windows servers. This is made easier if they use the tab completion features of their shells.

Bug ID: 137948

Description: After an application node is detached from a server, in the OGFS the file system under /opsw/Application/ is still accessible.

Platform: Independent

Subsystem: OGFS

Summary: In this situation, the user creates an application node under Application Servers in the SAS Web Client and then attaches the node to a managed server. In the Global Shell, the user cd's 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
```

Next, in the SAS Web Client, the user detaches the application node from the server. Here's the bug: In the Global Shell, the user 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: 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, as in the following 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: 141568

Description: Within 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: 144088

Description: SunOS OGFS: Hub start fails with ogfs_mount error in /var/adm/messages.

Platform: Sun OS

Subsystem: Global Shell

Symptom: The problem can be caused by setting the shell's cwd to the ogfs mountpoint (thereby making the mountpoint's vnode.v_count > 1). The full error is: ogfs: [ID 845410 kern.notice] ogfs_mount: error on overlay or vcount != 1 | vflag is already VROOT.

Workaround: Move the shell's cwd out of that directory, stop the Hub and start it again. It's not necessary to unload the kernel ogfs/ogdrv kernel modules or reboot the server.

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: 140696

Description: In rosh, an interactive Windows program hangs.

Platform: Windows

Subsystem: Global Shell

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

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

Bug ID: 143198

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

Platform: Linux

Subsystem: Global File System - backend

Symptom: TBD

Workaround: Log on as root to the OGFS server and enter the following commands:

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

Then, run the Opsware Installer again to install the OGFS.

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 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: After the cp command fails, make the target file writable, retry the cp command, and then make the file read-only 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: 148286

Description: Spoke client fails to reconnect to twist even after sshd is bounced.

Platform: Independent

Subsystem: Global File System - Spoke

Symptom: In Audit and Remediation, audits appear hung. In VAM, sitemaps appear hung. On the OGFS server, the “invalid value for select” message appears in the following log file:

Linux OGFS server:

```
/var/log/messages
```

Solaris OGFS server:

```
/var/adm/messages
```

Workaround: Restart sshd and then restart all of the twists in your core. For example:

```
/etc/opt/opsware/startup sshd restart
/etc/opt/opsware/startup/twist restartsync
```

Bug ID: 149155

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 needs to patch the passwd entry of the /etc/nsswitch.conf file. It is unable to do so if the entry is missing (as it is in some default Solaris configurations) or commented out.

This problem has the following symptoms:

- The SAS Client fails to initialize properly and issues "Spoke initialization failed. See Java console for details" message.
- 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 for a given site.)

If this is problem is detected after installing Opsware SAS, then fix /etc/nsswitch.conf on each OGFS server as described previously and then 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
```

NAS 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: After a port change, it took too long for NAS and SAS to reflect the correct configuration.

Subsystem: SAS Client - NAS Integration

Platform: Independent

Symptom: In a NAS/SAS integration, a managed server is connected to a switch. Unplug the network cable from the switch for this managed server. Plug the cable back in to the switch, to another port, on the same VLAN. Both SAS and NAS display the original configuration, instead of the correct (current) configuration. This can cause an "Unknown Configuration" and a duplex mismatch error 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

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, and retrieves and then caches customer information associated with the IP address of the request to the Software Repository server. Occasionally, this results in a `wordbot.accessDenied` error.

Workaround: None. This error is caused by a 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 sooner than ten minutes attempt to reprovision the same server, you will get a failure.

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

Bug ID: 138234

Description: Hardware registration information being deleted from server in server pool in SAS Web Client (unprovisioned server list in SAS Client)

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 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 be deleted.

Workaround: Re-boot the server into the server pool again.

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 behavior is not supported.

Bug ID: 143503

Description: OS Provisioning Process Completes Successfully but Remediation not Always Succeeding in Some Cases

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 prior to starting the remediate job. Permission problems, such as not having write access to the Customer assigned to the server by the OS Sequence, can cause this remediate job to silently fail.

Workaround: Make sure your user belongs to a group that has access to all servers and objects involved in the specific OS Provisioning process.

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: If you create an OS Installation Profile, and in the Remediate Policies task object, enable remediation, and in an Ad-Hoc Script 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: 143459

Description: If you provision a server that has customer "Not Assigned", and it got assigned a customer during provisioning, then you changed the server's customer back to "Not Assigned", it caused an error.

Platform: Any

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

Opsware Agent

Bug ID: 129395

Description: The Opsware Discovery and Agent Deployment (ODAD) feature in the SAS Client does not work in realms when the realm display name is different from the realm short name.

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

Platform: Independent

Symptom: The ODAD feature does not function because it cannot look up the Opsware Gateway information about the realm.

Workaround: None. Do not change the display name of a realm in the Opsware Command Center (web) UI so that it is different from the short name.

Bug ID: 129735

Description: Scanning a managed server opens the unmanaged server window.

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

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 Local Security Policy of the system is set in a particular way.

Subsystem: ODAD

Platform: Windows

Symptom: Some releases of Windows XP set the Local Security Policy in a particular way by default. 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".
5. Double click it.
6. Change to "Classic - local users authenticate as themselves".
7. Click Apply and then OK.

Bug ID: 137024

Description: Unable to install loopback adapters on a Windows 2003 64-bit AD Helper Server

Platform: Windows 2003 64 bit

Subsystem: Agent Deployment

Symptom: When you install the Opsware Agent Deployment Helper software policy on a Windows 2003 x64 server and configure the server as the Agent Deployment Helper server, deploying an Opsware Agent on a Windows server causes the Opsware Agent installation to fail with the error: "Unable to install loopback adapters."

Workaround: None. Using a Windows 2003 64-bit server as the server to run the Windows Agent Deployment Help is not supported.

Bug ID: 137558

Description: Using ODAD to install an Opsware Agent on a Windows server requires configuring a firewall port exception.

Platform: Windows XP with SP1 and Windows 2003 R2 with SP1

Subsystem: Opsware Discovery and Agent Deployment (ODAD)

Symptoms: ODAD uses NetBIOS to connect to Windows servers. If the Windows firewall on a server is enabled, ODAD cannot connect to the server unless the “Don't allow exceptions” option is disabled and a port exception for TCP 139 is enabled.

Workaround:

To disable the “Don't allow exceptions” option, perform the following steps:

1. From the Network Connections window, open the Properties page for the network connection. Access the Windows Firewall settings on the Advanced tab of the Properties window.
2. On the General tab, deselect the “Don't allow exceptions” option.

To enable an exception for port TCP 139, perform the following steps:

1. On the Windows Firewall window, select the Exceptions tab. Select the “File and Printer Sharing” service and click Edit. The Edit a Service window appears.
2. If not already selected, select the check box for port TCP 139. The default scope setting for this port is “Subnet.”

3. When the Opsware Agent Deployment Helper server and target Windows server are on different subnets, click the “Change scope” button and change the scope of the port to “Any computer” or enter a user specified custom list.
4. Click OK to save your configuration changes.

Bug ID: 149006

Description: Agent Upgrade Custom Extension causes multimaster conflicts.

Platform: Independent

Subsystem: Agent

Symptom: Running the Agent Upgrade Custom Extension causes an Agent to perform a hardware registration with a core, a transaction that updates the agent_version column in the core’s Model Repository. Some other process sets the agent_version column in the Model Repository of another core in the same multimaster mesh. The two transactions are propagated at about the same time, resulting in a conflict.

Workaround: For instructions on fixing multimaster conflicts, see the *Opsware® SAS Administration Guide*. To prevent this problem, only upgrade Agents on the managed servers that belong to the core you are logged in to with the SAS Web Client. To see which servers belong to a core, list the servers in the SAS Web Client, filtered by facility. (A facility belongs to a single core.)

Opsware API

Bug ID: 143527

Description: Authenticated user should not receive an AuthorizationException while calling a finder method.

Platform: Independent

Subsystem: Opsware SAS API

Symptom: Occurs when an authenticated user calls a finder that selects objects the user is not authorized to view, that is, the user does not have Read permission on the objects.

Workaround: Catch the AuthorizationException, which is the superclass of AuthenticationException.

Opsware Installer

Bug ID: 138694

Description: Upgrade failed due to an Oracle database problem.

Subsystem: Opsware Model Repository

Platform: Independent

Symptom: Oracle has a SYS.AUDIT_ACTIONS table. Oracle's default synonym AUDIT_ACTION is for SYS.AUDIT_ACTIONS. When the Model Repository creates the TRUTH.AUDIT_ACTIONS table, the synonym is changed to TRUTH.AUDIT_ACTIONS. When you upgrade Oracle software, Oracle will recreate 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 `ConnectionLimit` is set to a value that is too high for the operating system.

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, causing it to 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.

Bug ID: 147215

Description: Uninstallation of the core gateway does not remove certificates.

Subsystem: Opsware Gateway

Platform: Independent

Symptom: When the core Gateway is uninstalled using the Opsware Installer on a SAS core, it 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 Software Repository server 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.

Bug ID: 149282

Description: After a core upgrade, some managed servers become “Not Reachable”.

Subsystem: Opsware Installer

Platform: Independent

Symptom: After you upgraded a core, some managed servers that were “Reachable” became “Not Reachable” servers.

Workaround: Run the Communication test on the managed servers in the upgraded core to make them “Reachable” again.

Bug ID: 149334

Description: 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 with the following action file:

```
[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
```

Since the Opsware Installer is run from the primary distro, the content upload failed. The Opsware Installer prompted you for the upload distro, but did not accept the valid entry.

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

Bug ID: 149346

Description: The Opsware Installer does not give appropriate error messages when the action file is invalid.

Subsystem: Opsware Installer

Platform: Independent

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

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

```
Error Value: components
Exiting Opsware Installer.
```

Workaround: Revise the action file so that it is valid and then re-run the Opsware Installer.

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

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: Independent

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.

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: 149090

Description: Server search for custom fields with values fails.

Platform: Independent

Subsystem: SAS Web Client - Search

Symptom: In the SAS Web Client, when you search for SAS servers containing the following criteria,

Attribute = Custom Field

Operator = Equals

Value = <any numeric value such as 1>,

then the search returns the servers containing the custom fields associated with the value 1 and all other numeric values.

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.

Patch Management for Unix

Bug ID: 138929

Description: Unclear error message when base fileset and update fileset does not uninstall successfully during Patch remediation.

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: 139165

Description: APARs can be satisfied by both Update Filesets and Base Filesets.

Platform: AIX

Subsystem: SAS Client - Patch Management for Unix

Symptom: If the LPP containing the Base Fileset that satisfies an APAR is uploaded with the Import Package dialog, Opsware does not recognize that the Base Fileset satisfies the APAR. When you view the APAR properties, you will see “Unknown AIX Fileset” for the Base Fileset that was just uploaded.

Workaround: Upload the LPP containing the Base Fileset using the ocli with the -o option. Verify that the -C customer option specifies Customer Independent.

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

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: Characters that do not represent multi-byte characters display in the report description.

Workaround: See the information displayed in the Customer column.

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 files and 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: 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: 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: 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.

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).

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 HPUX depot patches in the SAS Client.

Subsystem: SAS Client - Software Management

Platform: HPUX

Symptom: After you import a HPUX 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 HPUX depot patch is not located in a folder.

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

1. Delete the HPUX depot patch using SAS Client.
2. From the Tools menu, select Update Cache.
3. Select the HPUX 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: 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 HPUX Products are not executed on the managed server during remediation.

Platform: Independent

Subsystem: Software Management

Symptom: For HPUX products, if you specify any pre or post install scripts on the Package window and then add the HPUX package to a software policy and remediate the server, then the HPUX 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, Software Compliance Scan is disabled for users in the Advanced Users Group.

Platform: Independent

Subsystem: Software Management

Symptom: After you upgrade to SAS 6.5, the Software Compliance Scan functionality is disabled for users in the Advanced Users Group in the SAS Client:

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: 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.

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: 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:

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

The followings topics in the Opsware SAS 6.5 User's Guide is updated with new information:

Code Deployment and Rollback

The Opsware Code Deployment and Rollback feature is not supported on VMware ESX.

Audit and Remediation

Snapshots results that were created previous to the SAS 6.5 release that contain either Microsoft IIS Metabase or COM+ rules cannot be packaged using the Visual Packager feature in SAS 6.5. You can still create the package, but none of the Microsoft IIS metabase of COM+ objects will be packaged and the objects will not get copied to the server onto which the package is installed.

To workaround this issue, recreate the snapshot in a new snapshot specification, and for COM+ objects, make sure you select the Archive all associated files option. Then you can create the package from the snapshot results.

Additional issues:

- If you take a snapshot of COM+ objects from a 32 bit Windows server, and you attempt to remediate the results using copy to onto a Windows 64 bit server, it may not work
- When remediating COM+ objects from a Snapshot or Audit Results using copy to, the SAS Client does not check the version of the COM+ object, and thus will always copy the object, whether or not there is any difference between them.

Creating a Dynamic Device Group

When a server matches the dynamic server group criteria, the server will appears quickly in the server group browser, under the server membership tab. However, there is a delay for the server to appear until the cache is reloaded in the following locations:

- From Devices ➤ Device groups ➤ Public, then clicking on the group ➤ Preview pane (Members)
- From double-clicking on a device group
- From selecting the Device Group Explorer window ➤ Summary tab (members)

Opsware Discovery and Agent Deployment Permissions

To use Opsware Discovery and Deployment (ODAD) in the Opsware SAS Client, you must have the permissions described in the Table 6-1.

Table 6-1: ODAD Feature Permissions

USER ACTION	FEATURE PERMISSION
Deploy (Install) Agent with ODAD	Allow Deploy Agent: Yes
Scan Network with ODAD	Allow Scan Network: Yes
View Servers Running Agents	Managed Servers and Groups

In addition to the feature permissions listed in the preceding table, you must have Read permissions on the following:

- Customer named Opsware
- Facility that has the servers targeted for Agent deployment.

To use ODAD on Windows managed servers, you also need Read permissions on the following:

- Customer that owns the server running the Windows Agent Deployment Helper (ADH)
- Facility that has the server running the Windows ADH
- Read permissions to the following directory in order to use the Windows ADH

```
/Opsware/Tools/Agent Deployment Helper
```


SAS Client Reports

The following new reports have been added to the SAS Client:

- Patch Compliance: Servers by Policy
- Software Compliance: Servers by Policy
- Server Audit Compliance
- Server Patch Policy Compliance
- Server Software Policy Compliance
- Server Patch Compliance Details
- Server Software Policy Compliance Detail

Updates to the Opsware SAS 6.5 Policy Setter's Guide

The following topic in the Opsware SAS 6.5 Policy Setter's Guide is updated to include the following information:

Software Policy Inclusion

If a Software Template contains sub policies then during remediation, Opsware does not consider the install order for the sub policies. For the software resources in a sub policy you can specify the install order and during remediation, all the software resources contained in the sub policies are then installed as per the install order.

Creating a Package

In the SAS Client, detaching a software policy containing a Windows zip package created using Visual Packager and then remediating the server does not remove the Windows zip package completely from the server. This behavior is observed if the directory containing the zip package is in use by some other applications.

Additionally, If you try to create a package selecting “all” of a category, such as All COM+ objects, All IIS Metabase, the entire registry, or even the entire file system of a server, you may not be able to successfully create the package because of file size limitations.

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

