Opsware® SAS 6.5.1.4 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 6.5.1.4

IN THIS CHAPTER

This section contains the following topics:

- Model Base Packages Functionality
- OS Installation Profile Package Parsing

Opsware Server Automation System (SAS) 6.5.1.4 automates critical areas of server and application operations – including the provisioning, patching, server and application configuration change management, compliance checking and reporting – across major operating systems and a wide range of software infrastructure and applications.

The following sections describe all new features and enhancements in the Opsware SAS6.5.1.4 release.

Model Base Packages Functionality

New for OS provisioning in Opsware SAS 6.5.1.4 is the ability to create software policies that model the base set of packages installed during OS provisioning.

During OS provisioning – after the base OS install, agent install, and reachability test, but before reconcile/remediate – a new script triggers software registration on the newly provisioned server, then models the installed packages as a software policy.

To activate this functionality, the server being provisioned must have a custom attribute defined (or inherited) named `model_base_packages`. The value for this attribute must either be empty or an absolute folder path to the name of the software policy to be created (or updated) with the package list.

If the `model_base_packages` value is empty, a software policy is created (or updated if it already exists) in the same folder as the OS Sequence. The software policy name will be the OS Sequence name plus `Base Packages`.

Each installed package that is successfully found in Opsware SAS is added to the list of software policy items. A list of package names and versions that were not found in SAS will be available as a custom attribute named `missing_packages` in the software policy. This policy is attached to the OS Sequence which has remediation enabled. Because the above occurs before remediation, this policy is included in the remediation, thus adopting the modeled packages since they are by definition already installed.

You should only specify the `model_base_packages` custom attribute value as empty when running OS Sequences from the SAS Client. When running OS Provisioning from the SAS Web Client, the `model_base_packages` custom attribute value must be the path to the Software Policy.

The only valid value for the `model_base_packages` custom attribute is the path to a Software Policy. For example:

```
/Customer/OS Baselines/Solaris 10 baseline Q4 2007
```

In this case, the Software Policy will be created at the specified path and with the specified name. Any folders that are missing will automatically be created. If the Software Policy already exists, it will be updated.

When run from the SAS Web Client Install OS wizard, the Software Policy will be attached to the server being provisioned. However, since the Install OS wizard triggers a legacy reconcile, remediate is bypassed so the policy will not be remediated.

Note that it is not necessary to use the Model Base Packages feature for every OS Provisioning job. It needs only to be used once after an OS Profile changes. From that point on, the Software Policy will be attached to the OS Sequence unless you remove it, and will be available for other servers as they are provisioned.

Model Base Packages Script Usage

The `model_base_packages.py` Command Engine script will function when called from another Command Engine script such as `provisionOS.py`. You can also run it as a standalone python2 pytwist script. The following are valid arguments when invoking the script:

```
model_base_packages.py --opsware-username you [--opsware-
password yourpass] --server <serverID> --ossequence
<ossequenceID> [--policy_path "/Some/Folder Path/Some Policy"]
```

Table 1-1: Options

ARGUMENT	DESCRIPTION
`--version`	Show the program version number and exit
`-h, --help`	Show this help message and exit
`-u OPSWAREUSERNAME, --opsware-username=OPSWAREUSERNAME`	Login username for SAS
`-p OPSWAREPASSWORD, --opsware-password=OPSWAREPASSWORD`	Login password for SAS
`-s SERVER, --server=SERVER`	Numeric Server ID of server to model
`m POLICYPATH, --policy_path=POLICYPATH`	Absolute path to the software policy that will model the packages
`-e OSSEQUENCE, --ossequence=OSSEQUENCE`	Numeric OS Sequence ID to link to the model software policy. If you specify an OS Sequence but not a policy path, the software policy will be created in the folder that contains the OS Sequence with the OS Sequence's name plus "Base Packages".

OS Installation Profile Package Parsing

For Opsware 6.5.1.4 only, OS Installation Profile package parsing code is restored. A package list attached to an OS Installation Profile can be parsed during upload.

Chapter 2: Platform and Environment Support for 6.5.1.4

IN THIS CHAPTER

This chapter contains the following topics:

- Supported Operating Systems for 6.5.1.4
- Supported Core Operating Systems for 6.5.1.4
- Operating System Deprecation and End of SupportOperating System Deprecation and End of Support
- Supported Installations and Upgrades for Opsware SAS 6.5.1.4
- Documentation for Opsware SAS 6.5.1.4

Supported Operating Systems for 6.5.1.4

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

Opsware Agents

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

Table 2-1: Opsware Agent Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR OPSWARE AGENT	VERSIONS	ARCHITECTURE
AIX	AIX 4.3 AIX 5.1 AIX 5.2 AIX 5.3	POWER POWER POWER POWER
HP-UX	HP-UX 10.20 HP-UX 11.00 HP-UX 11.11 HP-UX 11.23 (11i v2)	PA-RISC PA-RISC PA-RISC PA-RISC and Itanium PA-RISC and Itanium
Sun Solaris	Solaris 6 Solaris 7 Solaris 8 Solaris 9 Solaris 10 (Update 1, Update 2, Update 3)	Sun SPARC Sun SPARC Sun SPARC Sun SPARC Sun SPARC, 64 bit x86, 32 bit x86 and Niagara
Fujitsu Solaris	Solaris 8 Solaris 9 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

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

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

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

Opsware SAS Client

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

Table 2-2: SAS Client Supported Operating Systems

SUPPORTED OPERATING SYSTEMS FOR SAS CLIENT	VERSIONS	ARCHITECTURE
Windows	Windows Vista 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 for 6.5.1.4

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

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

Table 2-3: Opsware Core Supported Operating Systems

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

**Solaris 9 is currently supported, but is being phased out and will not be supported in a future major release.

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

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

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

Table 2-4: Opsware Satellite Supported Operating Systems

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

**Solaris 9 is currently supported, but is being phased out and will not be supported in a future major release.

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 6.5.1.4:

- 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 6.5.1.4:

- 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 6.5.1.4

The Opsware SAS 6.5.1.4 release supports the following installations:

- Upgrading a standalone core from Opsware SAS 6.5.1 to 6.5.1.4
- Upgrading a multimaster mesh from Opsware SAS 6.5.1 to 6.5.1.4
- Upgrading an Opsware Satellite from Opsware SAS 6.5.1 to 6.5.1.4

Documentation for Opsware SAS 6.5.1.4

This release comes with the following documentation:

- *Opsware SAS 6.5.1.4 Release Notes*
- *Technical Note: Opsware SAS 6.5.1.4 Upgrade Installation Instructions*
- *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 6.5.1.4 are compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 6.5.1.4 features with Opsware Agent versions prior to 6.5.1.4 yielded the following results for the features in the Opsware SAS Client:

SAS Client Features – Agent Compatibility

Opsware Agents 5.1 and Later

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

- Application Configuration Management
- Server Browser
- Opsware Global File System (OGFS)
- 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.

Opsware Agents 4.5 and 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: What's Fixed in Opsware SAS 6.5.1.4

IN THIS CHAPTER

This section list the bugs with a severity level of Critical or Major that are fixed in Opsware SAS 6.5.1.4. The fixed bugs listed affect the following Opsware components and functionality:

- Agent Installer
- DCML Export Tool (DET)
- Model Repository Multimaster Component
- OCC Web
- Opsware Agent
- OS Provisioning
- Patch Management
- Red Hat Network Import
- Server Management
- Virtualization

Agent Installer

Bug ID: 157390

Description: Agent kills non-Opsware `watchdog.exe` on installation.

Platform: Independent

Subsystem: Agent Installer

Symptoms: During Agent installation, non-Opsware `watchdog.exe` processes are incorrectly killed.

Resolution: Fixed

DCML Export Tool (DET)

Bug ID: 153422

Description: Quote Characters incorrectly translated to *&quot*.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptoms: During the CBT import of SuSE and Windows content, Quotes are being replaced with *&quot*.

Resolution: Fixed

Model Repository Multimaster Component

Bug ID: 149069

Description: Provide Tibco 7.5.4 support.

Platform: Independent

Subsystem: Model Repository Multimaster Component/TIBCO

Symptoms: Newer version of TIBCO is available.

Resolution: Fixed

OCC Web

Bug ID: 157033

Description: Manage Servers page takes 90+ seconds to load.

Platform: Independent

Subsystem: OCC

Symptoms: The main link to the Manage Servers page became slow to load after upgrade to 6.5.1.3.

Resolution: Fixed

Bug ID: 157036

Description: Displaying Public Groups and other group links is slow.

Platform: Independent

Subsystem: OCC

Symptoms: The main link to the public groups as well as displaying groups became slow after upgrade to 6.5.1.3.

Resolution: Fixed

Opsware Agent

Bug ID: 148871

Description: Agent returns incorrect chassis serial number on AIX.

Platform: IBM AIX

Subsystem: Agent

Symptoms: When querying for the AIX serial number, the serial number is returned formatted in a way that does not match the format of the serial number as it is printed on the hardware chassis label. But as I mentioned, changing the format of the serial number may be a change with quite a wide radius.

Resolution: Fixed

Bug ID: 148872

Description: Agent returns incorrect chassis serial number on HP-UX.

Platform: HP-UX

Subsystem: Agent

Symptoms: The method used to return the chassis serial number is incorrect.

Resolution: Fixed

Bug ID:148873

Description: Agent returns incorrect chassis serial number on Solaris.

Platform: Solaris

Subsystem: Agent

Symptoms: Some SPARC boxes do not return the correct serial number.

Resolution: Fixed

OS Provisioning

Bug ID: 155651

Description: Build Manager Miniagent protocol can become out of sync due to minimal network traffic.

Platform: Independent

Subsystem: OS Provisioning

Symptoms: The build manager protocol makes use of low-level timeouts for basic message processing. This makes the protocol very susceptible to getting out of sync even if there is only minor network congestion.

The specific network congestion involves a problem that causes the TCP/IP stack of the kernel where the miniagent is running to hang at random intervals for random periods of time. Typically between 5-120 seconds. If a hang occurs at the right time during one of the timeout intervals of the `BM<->MA` protocol, then the protocol can get out of sync.

Resolution: Fixed

Bug ID: 155652

Description: The Build Manager can crash due to corrupt data from the Miniagent.

Platform: Independent

Subsystem: OS Provisioning

Symptoms: A miniagent responds to `-READ-` operations from the Build Manager by returning a 12 byte, 3-int header followed by the data being read. The third integer in this header represents the number of bytes in the data payload of the response message from the Miniagent. Occasionally, the header data can become corrupted due to the protocol getting out of sync.

Resolution: Fixed

Bug ID: 155969

Description: The Build Manager can deadlock due to synchronization problems.

Platform: Independent

Subsystem: OS Provisioning

Symptoms: Due to some unnecessary synchronization methods, the Build Manager could deadlock during concurrent provisionings.

Resolution: Fixed

Bug ID: 156284

Description: Cannot parse OS Provisioning installation profiles for modeling OS Provisioning packages.

Platform: Independent

Subsystem: OS Provisioning

Symptoms: In Opsware SAS 4.x-5.x, when a user uploaded a jumpstart profile (Solaris), kickstart profile (Red Hat), or autoinst.xml (SuSE), parsing/interpreting logic inside the Web Services Data Access Engine would translate this text-based profile into a list of individual packages that the OS installer could install. These packages would be automatically modeled when attached to an OS Installation Profile on the Packages tab of the OCC Web Client.

During provisioning, the native OS installer would install these packages and, because they were also modeled in SAS, they would be *adopted* meaning you could then consider them during a full reconcile and reconcile would ensure that the servers remain at that initial state.

Resolution: Fixed

Bug ID: 156716

Description: Creating Linux OS Profile Fails

Platform: Independent

Subsystem: OS Provisioning

Symptoms: Import Linux media into the core. From the OCC, select **Prepare OS** and enter the required data. Select a `ks.cfg` file to upload, then click **Upload**. The process fails with the following error message:

```
Error ID: 12970135
Error Name: Twist Method Error
Exception Info: com.opsware.exception.TwistException
```

Resolution: Fixed

Bug ID: 157819

Description: `model_base_packages` does not handle RPMs with just release different.

Subsystem: OS Provisioning

Platform: Linux

Symptom: Although certain Windows patches have been installed on a server, the server is still shown as non-compliant.

Resolution: Fixed

Bug ID: 157910

Description: SLES 9 `base_packages` software policy `missing_packages` custom attribute shows packages that were Installed on the Server.

Subsystem: OS Provisioning

Platform: Linux

Symptom: SLES9 installs correctly, the `base_packages` software policy is created and remediated to the server, but the list of missing packages includes packages that the server shows as "Installed."

Resolution: Fixed

Bug ID: 157992

Description: Provisioning from the web with `base_packages` CA set, fails.

Subsystem: OS Provisioning

Platform: Independent

Symptom: pxe-boot server with Linux4. Create OS with CA `model_base_packages` set to `SW_Policies/RH4AS_SW_Policy1` where the path exists. Run **Install OS** on the server.

Results:

- The server is provisioned with the correct OS
- the installation fails with the error:

```
Name: Error during provisionOS
Description: An unidentified error occurred during
provisionOS.
```

- The expected software policy is created, but it contains no packages.

Resolution: Fixed

Patch Management

Bug ID: 156164

Description: Patch compliance shows *Non-compliant* when it should show *Compliant*.

Subsystem: Patch Management

Platform: Independent

Symptom: Although certain Windows patches have been installed on a server, the server is still shown as non-compliant.

Resolution: Fixed

Red Hat Network Import

Bug ID: 156706

Description: Red Hat Network Import login failure prevents package download.

Platform: Independent

Subsystem: Red Hat Network Import

Symptoms: Red Hat Network Import fails to download packages because the package download form is submitted to the wrong URL. The login form's action attribute is ignored.

Resolution: Fixed

Bug ID: 157223

Description: Red Hat Network fails due to policy description exceeding 1000 bytes (with Oracle 9i).

Platform: Linux

Subsystem: Red Hat Network Import

Symptoms:

Resolution: Fixed

Server Management

Bug ID: 153708

Description: Unprovisioned server view does not show MAC Address until you browse away from and back to the view

Platform: Independent

Subsystem: Server Management: Managed Servers

Symptoms: Browse to **Devices** --> **Unmanaged Servers** in the NGUI. Add MAC Address to the column specification. Have a system join the server pool. Refresh the cache to show the system. The system does not show a MAC address. Refreshing the cache does not correct the problem, but if you drill into the details for the server, the MAC address is listed.You can also browse away and back to Unmanaged Servers and the MAC now displays correctly.

Resolution: Fixed

Virtualization

Bug ID: 157154

Description: Clicking on Virtualization while the cache is loading causes OutOfMemory error and a crash.

Platform: Independent

Subsystem: Virtualization

Symptoms: Launch the Virtualization interface. Before the server cache finishes updating, click on Virtual Servers.

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

Also, when a list of Virtual Servers is retrieved, performance is slow.

Resolution: Fixed

Chapter 5: Known Problems, Restrictions, and Workarounds in Opsware SAS 6.5.1.4

IN THIS CHAPTER

This chapter describes workarounds for known problems in Opsware SAS 6.5.1.4. These descriptions are arranged by the following features:

- Application Configuration
- Audit and Remediation
- DCML Exchange Tool (DET)
- Global Shell
- Jobs and Sessions
- 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
- Virtualization
- Visual Application Manager (VAM)
- Visual Packager

Application Configuration

Bug ID: 137456

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

Platform: Independent

Subsystem: Application Configuration

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

Workaround: None

Bug ID: 138610

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

Platform: Independent

Subsystem: Application Configuration - Device Groups

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

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

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

Bug ID: 139042

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

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rule

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

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

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

Audit and Remediation

Bug ID: 137898

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

Platform: Independent

Subsystem: Audit and Remediation

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

Workaround:

1. Get the Windows utilities (showpriv.exe, ntrights.exe, auditpol.exe) from the Microsoft Windows 2000 Resource Kit.
2. Install the OCLI on a UNIX server managed by Opsware, or on an Opsware core server.

3. Copy the Windows utilities to /var/tmp on the UNIX server.
4. Make sure /opt/opsware/agent/bin is at the beginning of the PATH

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

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

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

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

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

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

   b) Go to 'Patch Settings'

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

Bug ID: 137901

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

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rules

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

Workaround: Avoid using “does not contain” more than once in an application configuration Audit and Remediation rules.

Code Deployment and Rollback

Bug ID: 145470

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

Platform: VMWare ESX 3

Subsystem: Code Deployment and Rollback

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

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

DCML Exchange Tool (DET)

Bug ID: 130600

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

Platform: Independent

Subsystem: DET Import

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

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

Bug ID: 138949

Description: Some imports fail if Microsoft patches are missing.

Platform: Windows

Subsystem: DET

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

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

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

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

Bug ID: 135494

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

Platform: Independent

Subsystem: DET

Summary: 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 shipped with the product includes a carriage return (`\r`), which appears 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: Users can edit their `.bash_profile` and change the PS1 setting to:

```
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.

For example:

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

Workaround: 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 a "`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
```

Jobs and Sessions

Bug ID: 139762

Description: Different IDs are shown for the same job on NGUI and OCC web.

Subsystem: Jobs and Sessions

Platform: Independent

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

For example, NGUI shows Job 13880001 which is the same as Job 13930001 on OCC.

Workaround: None

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

Bug ID: 149729

Description: OS provisioning using authenticated windows share for media.

Subsystem: OS Provisioning

Platform: Windows

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

Example:

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

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

Workaround: Edit the file:

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

and replace these lines:

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

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

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

Bug ID: 157913

Description: Invalid `base_packages` value leads to unclear error message.

Subsystem: OS Provisioning

Platform: Independent

Symptom: When running an OS Sequence on a server where the specified `model_base_packages` value is invalid, the OS Provisioning job completes successfully. However, the `base_packages` Software Policy is not created and no error message is displayed.

Workaround: Specify a valid `model_base_packages` value and run the OS Sequence again.

Bug ID: 158071

Description: Prepare Solaris x86 operating system on Solaris 10 Core - no packages are displayed in the Opsware SAS Client.

Subsystem: OS Provisioning

Platform: Sun Solaris

Symptom: You import Solaris 10x86 media to a Solaris 10 core and run Prepare OS. The OS Profile is created successfully, however, no packages are displayed under the Packages tab in the Opsware SAS Client.

Workaround: Specify the IP address of the server on which the media you want to import is stored rather than the hostname.

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 s 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” and then double click it.
5. Change to “Classic - local users authenticate as themselves”.
6. Click **Apply** and then **OK**.

Bug ID: 118907

Description: matruska.exe/unzip.exe error when c:\ is specified as the unzip directory

Platform: Independent

Subsystem: Opsware Agent

Symptoms: Some combination of unzip.exe and matruska.exe causes the unzip operation to fail when c:\ is specified as the unzip directory. If during reconcile, the OCC reports an out of space error in at least one of the two cases (the error from the command line is different depending on if c:\ is quoted or not in the invocation of matruska.exe).

Workaround: None. To be fixed in a later release.

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: 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: 141338

Description: Unable to delete OS Installation Profiles in the SAS Web if Profile references a policy

Platform: Any

Subsystem: SAS Web - OS Provisioning

Symptom: If you attempt to delete an OS Installation Profile in the SAS Web Client that references a policy (for example: an OS Sequence), you will not be able to delete it.

Workaround: Delete or detach any policies that the OS Installation Profile references, and then it can be deleted.

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.

Bug ID: 138063

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

Platform: All

Subsystem: Patch Jobs - Upgrade

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

Workaround: None

Bug ID: 149449

Description: Ad hoc Patch installation job aborted if one of the patches selected to install is deleted from core

Platform: Any

Subsystem: Patch Management

Symptom: If you schedule an ad hoc patch installation job to run and set the job to "continue if an error occurs," and one of the patches selected in the job is deleted before the job runs, the entire job will be aborted.

Workaround: Make sure that none of the patches selected to run in the job is deleted before the job runs, or reset the job to exclude the missing patch.

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

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

Bug ID: 134581

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

Platform: Independent

Subsystem: SAS Client - Reports

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

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

Bug ID: 136029

Description: The Action menu is disabled in Reports.

Platform: Independent

Subsystem: SAS Client - Reports

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

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

Bug ID: 143410

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

Platform: Windows

Subsystem: SAS Client - Reports

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

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

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

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

Bug ID: 147275

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

Subsystem: SAS Client - Reports

Platform: Independent

Symptom: You tried to export the following reports to HTML, XLS, or PDF 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: 150436

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

Platform: Any

Subsystem: SAS Client Reporting - Compliance - Patch Policies

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

Workaround: None

Bug ID: 149277

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

Subsystem: SAS Client - Reports

Platform: Independent

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

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

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

Bug ID: 150508

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

Platform: Any

Subsystem: SAS Client - Reports

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

Workaround: None.

Software Management

Bug ID: 133443

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

Subsystem: SAS Client - Software Management

Platform: Independent

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

Workaround: None.

Bug ID: 136715

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

Subsystem: SAS Client - Software Management

Platform: Independent

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

Workaround: Close the Package window and open it again.

Bug ID: 137989/138896

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

Subsystem: SAS Client - Software Management

Platform: Independent

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

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

Bug ID: 138934

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

Subsystem: SAS Client - Software Management

Platform: Independent

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

Workaround: None.

Bug ID: 139254

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

Platform: Independent

Subsystem: Software Management

Symptom: If you have Write permission on a folder, and No Read or Write permissions on the objects (such as packages, software policies) contained in the folder, then you can view the packages and software policies in the folder. You will not be able to perform any

actions on the Folder objects. If you move or cut/paste the folder to another location, then the packages and software policies in the folder will also be moved or cut and then pasted to the destination folder.

Workaround: None.

Bug ID: 139040

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

Subsystem: SAS Client - Software Management

Platform: Independent

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

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

Bug ID: 139046

Description: Unable to delete 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: 146298

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

Platform: Independent

Subsystem: Software Management

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

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

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

Bug ID: 147577

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

`Platform:` Independent

Subsystem: Software Management

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

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

Bug ID: 148745

Description: Pre or Post install scripts specified for 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 6.5.1.4, Software Compliance Scan is disabled for users in the Advanced Users Group.

Platform: Independent

Subsystem: Software Management

Symptom: After you upgrade to SAS 6.5.1.4, 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: 148777

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

Platform: Independent

Subsystem: Software Management

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

“Twist exception while getting parent folder”

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

Bug ID: 148797

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

Platform: Independent

Subsystem: Software Management

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

Bug ID: 149043

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

Platform: Red Hat Linux

Subsystem: Software Management

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

Workaround: None.

Bug ID: 149093

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

Platform: Independent

Subsystem: Software Management

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

Workaround: None.

Bug ID: 157932

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

Platform: Independent

Subsystem: Software Management

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

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

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).

Visual Application Manager (VAM)

Bug ID: 143148

Description: HP-UX Process Family Limitation

Platform: HP-UX

Subsystem: Visualizing Process Families for HP-UX

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

Workaround: None.

Visual Packager

Bug ID: 139169

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

Platform: Windows

Subsystem: Visual Packager

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

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

Bug ID: 139506

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

Subsystem: SAS Client - Visual Packager

Platform: Independent

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

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

Bug ID: 143744

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

Platform: AIX

Subsystem: SAS Client - Visual Packager

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

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

Workaround: None.

Bug ID: 143744

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

Platform: AIX

Subsystem: Visual Packager Backend

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

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

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

Bug ID: 149117

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

Platform: Independent

Subsystem: Visual Packager

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

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

1. Register the DLL on the source server.

2. Create a package with the COM+ objects.
3. Attach the software policy to the server.
4. Remediate the server.

Chapter 6: Documentation Errata

IN THIS CHAPTER

This chapter contains the following topics:

Updates to the Opsware SAS 6.5.13 Release Notes

The 6.5.1.3 Release Notes state that Opsware SAS supports HP-UX 11i v3 on managed servers. This is in error. Opsware SAS 6.5.1.3 does not provide support for HP-UX 11i v3.

Update to the Opsware SAS User's Guide: Application Automation, Chapter 9: Operating System Provisioning

Red Hat Linux Support

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

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

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://support1.opsware.com/index.php

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

