Opsware® SAS 6.0.2 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: Introduction to Opsware SAS 6.0

IN THIS CHAPTER

This chapter contains the following topics:

- Opsware SAS 6.0 Overview

Opsware SAS 6.0 Overview

Opsware Server Automation System (SAS) 6.0 provides a core set of features that automate critical areas of server and application operations – including the provisioning, deployment, patching, and change management of servers – across major operating systems and a wide range of software infrastructure and application products. The introduction of the Visual Application Manager (VAM) helps you understand and manage the operational architecture and behavior of distributed business applications in your IT environment.

Additionally, Opsware SAS supports the NAS Integration feature so that you can examine detailed information about managed servers and the network devices connected to them and determine how they are related.

Opsware SAS 6.0 provides new features, performance enhancements and several bug fixes. This document describes the new features found in this release, and provides information about the most significant bug fixes, and, in some cases, workarounds for known problems.

Opsware SAS 6.0 includes the following new features:

- The Compliance Dashboard
- The Visual Application Manager (VAM)
- Layer 2 connection visibility (requires Integration with Opsware NAS)
- Network device access (requires Integration with Opsware NAS)

  See the *Opsware® SAS Planning and Installation Guide* for information about setting up the NAS Integration feature.

- Application infrastructure change history
- Automated configuration mismatch detection
- The Opsware Network

See *Opsware® SAS 6.0.1 Release Notes* for information about each of these new features.

See *Opsware® SAS 6.0.1 Release Notes* for information about the operating systems supported in this release.

Chapter 2: What's New in This Release

IN THIS CHAPTER

This chapter contains the following topics:

- New Features in Opsware SAS 6.0.2

See *Opsware® SAS 6.0.1 Release Notes* for information about the new features in Opsware SAS 6.0.1

New Features in Opsware SAS 6.0.2

Content Migration for Opsware SAS 6.0.2

In Opsware SAS 6.0, enhanced software management functionality is available as part of the SAS Client. The Software Management feature in the SAS Client replaces the node-based Software Tree accessible from the SAS Web Client.

After upgrading an Opsware SAS core to 6.0.2, you run the Software Migration Tool to migrate Software Tree nodes and package information to the Library in the SAS Client. Running the Software Migration Tool on your upgraded SAS core allows you to use the new software management features with your existing data. After the migration, your Software Tree data and package information appear in the SAS Client under the Migrated folder in the Library.

Because the new Software Management functionality and the old functionality are both available after upgrading to Opsware SAS 6.0.2, customers can choose the best time for them to migrate completely their Software Tree data and package information.

Chapter 3: What's Fixed in Opsware SAS 6.0.2

IN THIS CHAPTER

This chapter contains bugs have a severity level of Critical or Major and are fixed in Opsware SAS 6.0.2 These descriptions are arranged by the following features:

- OS Provisioning
- Software Management

See *Opsware® SAS 6.0.1 Release Notes* for the bugs fixed in Opsware SAS 6.0.1.

OS Provisioning

Bug ID: 140024

Description: When you copied any Windows x64 R2 media to a Solaris media server and ran the import_media script, the script failed with the following error:

```
Detecting OS Version...
File "./util/import_media.py", line 2641, in ?
File "./util/import_media.py", line 1852, in __init__
File "./util/import_media.py", line 724, in __init__
File "./util/import_media.py", line 1865, in getPlatform
File "./util/import_media.py", line 1951, in _getMediaVersion
File "./util/import_media.py", line 1838, in _readFileLines
```

Subsystem: OS Provisioning

Platform: Solaris

Resolution: Fixed.

Software Management

Bug ID: 139953

Description: Migration Script does not check for the length of the package name if it exceeds over the database character limit.

Subsystem: Software Management - Content Migration

Platform: Independent

Symptom: During content migration, if a package of the same name exists in the SAS Client and the SAS Web client, the migration script appends the package unit name in the SAS client with the version number. This may result in exceeding the database limitation for the unit name of the package. As a result there is an Illegal Value Exception during migration.

Resolution: Fixed.

Bug ID: 139995

Description: Migration Script does not check for folder_unit_registry constraint violation.

Subsystem: Software Management - Content Migration

Platform: Independent

Symptom: During content migration, if a package name in the SAS Web Client and the SAS Client contains the same unit_file_name, then you receive an Illegal Value Exception during migration. This exception is thrown since the folder_unit_registry constraint is violated.

Resolution: Fixed.

Chapter 4: Known Problems, Restrictions, and Workarounds in Opsware SAS 6

IN THIS CHAPTER

This chapter describes workarounds for known problems in Opsware SAS 6. These descriptions are arranged by the following features:

- Application Configuration
- Audit and Remediation
- DCML Exchange Tool (DET)
- Global Shell
- Intelligent Software Module (ISM) Development Kit
- Operating System Provisioning
- Opsware Agent
- Opsware Installer
- Opsware SAS Client
- Patch Management
- Reports
- Software Management
- Visual Application Manager
- Visual Packager

Application Configuration

Bug ID: 134791

Description: Error dialog displays when selecting Configured Application in some Device Explorer windows.

Platform: Independent

Subsystem: Application Configuration/Device Explorer

Symptom: If you open a Device Explorer for a server that belongs to a facility whose Name and Short Name do not match, and select Configured Application in the View pane, then an error dialog will display.

Workaround: The configured application configurations will be viewable in the Device Explorer if the Name and Short Name of the facility the server belongs to matches.

Bug ID: 137456

Description: Preserve format does not preserve comments when the 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: 138504

Description: Performing an application configuration data-manipulation run script concurrently by two users will only execute successfully for one of the users.

Platform: Independent

Subsystem: Application Configuration

Symptom: If you create an application configuration that contains a data manipulation script, attach the application configuration to a server, and two users both try to perform a 'run script' at the time, only one of the user's script execution will succeed. The script should queue and both execute, one after the other.

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: 139644

Description: When upgrading from Opsware SAS 5.2 to SAS 6.0.1, Application Configuration recurring push jobs become un-editable.

Platform: Independent

Subsystem: Application Configuration

Symptom: If you are upgrading from Opsware SAS 5.2 to SAS 6.0.1, any recurring application configuration push jobs that were created in SAS 5.2 will not be editable in the SAS 6.0.1 version.

Workaround: Delete the migrated push jobs that are uneditable and create new ones.

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 IDs: 137901, 137904

Description: Application Configuration audit rules operator “does not contain” should not be used twice in an audit rule.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: In the Application Configuration rule of the Audit and Remediation feature, “does not contain” will not work as expected if used twice in a single rule.

Workaround: Do not create a rule that uses two instances of “does not contain”.

Bug ID: 137898

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

Platform: Independent

Subsystem: Audit and Remediation

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

Workaround:

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

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

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

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

oupload  -C"Customer Independent"  -t"Windows Utility"  -
O"Windows 2003"  --old  /var/tmp/auditpol.exe
```
6. Perform the following steps to validate the file upload:

   a) Using OCCC, 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: 138164

Description: SAS 5.0 Audit Results migrated to SAS 6.0 will show value of -1 for all differences in audit results object list in the SAS Client

Platform: Independent

Subsystem: Audit Results

Symptom: If you upgrade Opsware SAS from 5.0 to 6.0, any audit you created and ran in SAS 5.0 will display audit result differences in the main audit results list with a value of -1, no matter how many actual differences were found in the original audit. For example, if you create and ran an audit using SAS 5.0 and the results produced 5 differences between the audit rule and the target server, when you upgrade SAS to 6.0, the differences will display incorrectly as -1 in the audit results object list Differences column in the SAS Client.

To see this, select audit results from the navigation pane, select an operating system (Windows or UNIX) and in the contents pane, the differences column will show -1 for any SAS 5.0 migrated audit results.

Workaround: Open the individual audit results and the correct number of differences will display in the audit results window.

Bug ID: 135855

Description: Copy To for Non Existent Windows Services on Target Doesn't Provide Feedback that Remediation/Copy To Did Not Work

Platform: Windows

Subsystem: Audit and Remediation - Audit and Snapshot

Symptom: If you create an audit or snapshot specification that contains a rule for a Windows Service that does not exist on the target, or has a dependency on another service, and in the Audit Results or Snapshot you try to remediate (audit) or use “copy to” (snapshot), the remediate or copy to will not work, but you will not see an error messages stating failure to remediate/copy to.

Workaround: None.

Bug ID: 137901

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

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rules

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

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

Bug ID: 139346

Description: Cannot use Windows drive:\directory\filename syntax when creating an Audit and Remediation application configuration rule.

Platform: Windows

Subsystem: Audit and Remediation Application Configuration Rules

Symptom: If you attempt to create an Application Configuration rule inside an audit or snapshot, and the path to the application configuration template file uses the standard Windows pathname convention, you will not be able to load the template and cannot create the rule.

Workaround: Use the Unix file system format for the application configuration rule. For example, "/c/test files/insight.ini".

Bug ID: 140121

Description: Predefined custom rules disappear when an Audit Result is deleted.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: In the SAS Client, when you delete an Audit Result that includes any predefined custom rules, the predefined custom rules are also deleted.

Workaround: After you delete an Audit Result in the SAS Client, re-upload the predefined custom rules .

Or

Avoid deleting any Audit Results that includes predefined custom rules.

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: 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 OCC Client you can use the Remote Terminal feature to open a terminal window for a Unix or Windows server and the Global Shell feature to open a terminal window for Opsware Global File System (OGFS). If the Remote Terminal session or the Global shell session for server times out or is disconnected, the following error displays:

An internal error has occurred. See the console log for details.

Workaround: Restart the OCC Client and then open a new terminal window for a Windows or Unix server.

Bug ID: 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: 132935

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

Subsystem: SAS Client - Global Shell

Platform: Independent

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

Workaround: Enter the following command:

```
chmod 700 /var/opt/OPSWmnt/audit/streams/<server>
```

Bug ID: 137220

Description: Opsware PAM module requires use of -r option for passwd program.

Subsystem: OGFS Backend

Platform: Linux

Symptom: This problem occurs on the core server where the OGFS is installed, when you log into the core server and try to change the password of a Unix user with the passwd program. If you do not specify -r for passwd, the following error appears:

"Unsupported nsswitch entry for passwd:. Use -r repository. Unexpected failure. Password file/table unchanged." The Opsware PAM module is installed on the core server where the OGFS component is installed. Because the Opsware PAM module alters /etc/nsswitch.conf, the passwd program needs the -r option to function correctly.

Workaround: Specify the -r option, for example:

```
% passwd -r files username
```

Bug ID: 136129

Description: Cannot browse contents of a Windows server as Administrator if Administrator password has zero length.

Subsystem: Global File System Backend

Platform: Windows

Symptom: In the Device Explorer of the SAS Client, you cannot browse the file system, COM+ catalog etc. as a user other than LocalSystem (if such a user is defined). You can see the userid, but the File System, Windows COM+ Objects, and 'Windows Registry folders will not expand. In a Global Shell session, you cannot browse the file system, registry, etc. of the Windows server; doing so generates the error message, "Input/output error."

Workaround: Assign a password of non-zero length to Administrator, or, browse the server as another user.

Bug ID: 137821

Description: Cannot write to Solaris attribute files in OGFS from a Global Shell session.

Subsystem: SAS Client - Global Shell

Platform: Solaris

Symptom: In a Global Shell session, try to write to an attribute file (in attr subdirectory) of a Solaris managed server. The contents of the file are either unchanged or emptied. Reading attribute files works correctly.

Workaround: Change server attributes with the Opsware SAS Client.

Bug ID: 1369095

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

Platform: Independent

Subsystem: Global Shell

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

Workaround: User can edit their .bash_profile and change the PS1 setting to the following:

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

Bug ID: 133316

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

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

Subsystem: Global Shell

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

Here's an example that reproduces this problem:

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

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

Bug ID: 137948

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

Platform: Independent

Subsystem: OGFS

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

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

Next, in the SAS Web Client, the user detaches the application node from the server. Here's the bug: In the Global Shell, the user can still access the server's file system under the detached node.

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

Intelligent Software Module (ISM) Development Kit

Bug ID: 135455

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

Platform: 64-bit Windows

Subsystem: ISM

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

Workaround: None

Operating System Provisioning

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: 137956

Description: A Red Hat Linux Enterprise Linux 4 AS VMware Guest server cannot be provisioned using the default vmxbuslogic SCSI controller

Platform: Red Hat Linux Enterprise Linux 4 AS

Symptom: If you attempt to provision a VMware guest server with the Red Hat Linux Enterprise Linux 4 AS operating system and the target server is using a vmxbuslogic SCSI controller, the provisioning job will not succeed because of a Red Hat Linux compatibility limitation.

Workaround: When creating the virtual machine, select the LSI Logic SCSI adapter. Refer to the VMware guest OS installation release notes for details and updated and specific server installation notes located at http://pubs.vmware.com/guestnotes/wwhelp/wwhimpl/js/html/wwhelp.htm.

Bug ID: 138810

For an explanation of this bug, see “Bug ID: 138810” on page 38 in the section “Patch Management”.

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: 138943

Description: Creating a Linux boot disk for Itanium 64-bit servers causes errors and does not boot.
Platform: Linux

Subsystem: OS Provisioning

Symptom: If you attempt to create a Linux boot disk for an Itanium 64 bit server and you are not logged in as root, you will get a series of errors and not be able to create the boot disk.

Workaround: None.

Bug ID: 139498

Description: OS Provisioning with Windows 2003 sometimes fails when mounting Win 2k3 media with a "duplicate workgroup or computer name" error

Platform: Windows 2003

Subsystem: Windows OS Provisioning

Symptom: In some cases, provisioning a server with Windows 2003 sometimes will fail when mounting Win 2k3 media and display a "duplicate workgroup or computer name" error.

Workaround: When you boot opsware DOS image, in the menu of emm386 choices, accept the default choice: 1) no emm386.

Bug ID: 139839

Description: Provisioning Windows XP Service Pack 2 (SP2) using an OS sequence is not working, where the OS sequence consist of XP RTM plus XP SP2 with unit post script.

Platform: Windows XP SP2

Subsystem: OS Provisioning Remediation

Symptom: If you attempt to provision a Windows XP SP2 server using an OS sequence that contains XP RTM plus XP SP2 with unit post script, the server will not reboot and the session will time out after 4 hours.

Workaround: You can either use an OS installation profile for the OS sequence that has Windows XP SP2, and not use the RTM media. Or, you can disable remediation in the OS sequence and perform the remediation after the OS installation has completed.

Bug ID: 139352

Description: OS sequences do not allow Software Policies that are "Platform = Independent"

Platform: Independent

Subsystem: OS Provisioning - OS Sequences

Symptom: If you create a software policy that is Platform Independent and then attempt to add that software policy to an OS sequence, it will not appear in the list of policies to attach to the OS sequence.

Workaround: None

Bug ID: 140524

Description: In a multimaster mesh if the content upload upgrade was performed on only one core, and a Red Hat OS media was imported only on the other core before the upgrade, then the Red Hat OS Provision with that particular OS media will fail.

Platform: Linux

Subsystem: OS Provisioning

Symptom: If a Linux media was only imported in the core where the content upload was not performed, then the new stage2.img file is not updated after the multimaster mesh is upgraded to 6.0.2. This results in the OS Provisioning Job to fail with the following error:

```
The Red hat Enterprise Linux installation tree in that directory
does not seem to match your boot media
```

This behavior is only observed in a multimaster mesh where the content upload upgrade was performed on only one core, and a Red Hat OS media was imported on the other core of the mesh before the upgrade.

Workaround: After you upgrade to Opsware SAS 6.0.2, perform the content upload upgrade to all the cores in a multimaster mesh.

Bug ID: 140685

Description: dhcpd fails to start after upgrading to Opsware SAS 6.0.2

Platform: Independent

Subsystem: OS Provisioning

Symptom: After upgrading to Opsware SAS 6.0.2, the subnet definitions in the dhcpd.conf are not saved and the dhcpd fails to start.

Workaround: Before you upgrade to Opsware SAS 6.0.2, remove or rename the file `/etc//opt/opsware/dhcpd/dhcpd.conf.rpmsave` if it exists.

You can also retrieve any lost configuration from the configuration file archive located at

`/var/opt/opsware/install_opsware/config_file_archive`

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: 137558

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

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

Subsystem: Opsware Discovery and Agent Deployment (ODAD)

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

Workaround:

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

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

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

1. On the Windows Firewall window, select the Exceptions tab. Select the “File and Printer Sharing” service and click Edit. The Edit a Service window appears.
2. If not already selected, select the check box for port TCP 139. The default scope setting for this port is “Subnet.”
3. When the Opsware Agent Deployment Helper server and target Windows server are on different subnets, click the “Change scope” button and change the scope of the port to “Any computer” or enter a user specified custom list.
4. Click OK to save your configuration changes.

Bug ID: 139652

Description: OS provisioning on Windows 2003 x64 fails intermittently on files during untar phase

Platform: Windows 2003 x64

Subsystem: Windows OS Provisioning

Symptom: During the OS Provisioning of Windows 2003 x64 Standard Edition, the extraction of the i386.tar file during the DOS phase of the setup can fail on some files in certain hardware configurations. It is not always consistent on the files it will fail on. Consequently the Windows install may, or may not be affected, depending on the files missed during the extraction.

Workaround: None available at this time. Please contact Opsware support if you are experiencing this issue.

Bug ID: 137024

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

Platform: Windows 2003 64 bit

Subsystem: Agent Deployment

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

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

Opsware Installer

Bug ID: 137740

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

Subsystem: Opsware Global File System Server (OGFS)

Platform: Independent

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

Workaround:

1. On the server running the OGFS component, run the following command to determine whether the OGFS started:

   ```
   [ -d /var/opt/opsware/ogfs/mnt/ogfs/.authenticate ] &&
   echo DOWN || echo UP
   ```

   If the OGFS did not start, the command displays the following output: DOWN.

2. Start the OGFS component by performing the following steps:

   a) Log on as root to the server running the OGFS component.

   b) Enter the following command to start the OGFS component:

   ```
   /etc/init.d/opsware-sas start hub
   ```

Bug ID: 138633

Description: Opsware SAS core un-installation fails when the binaries for the Opsware Installer are removed from the directory /var/tmp/oitmp

Platform: Unix

Subsystem: Opsware Installer > SAS Core Un-installation

Symptom: Running the Opsware Installer to uninstall a SAS core fails.

Workaround: None. Do not remove the directory /var/tmp/oitmp before uninstalling an Opsware SAS core. If you have already removed the directory, copy it from another core in your Opsware SAS multimaster mesh and replace it before proceeding with the un-installation.

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: 135932

Description: Search on an Audit also displays the source name of the Audit.

Subsystem: SAS Client - Search

Platform: Independent

Symptom: In the SAS Client when you search for the item Audit using any of the following attribute values,

Source / Target Server

Source/Target Server Asset Tag

Source/Target Server Serial Number

Source/ Target Snapshot Name

the results displayed contains all the audits which match the attribute value. In the results the source name of the audit is also displayed in the Source column. The source of the audit could be a server or a snapshot or none.

Workaround: None

Bug ID: 137634

Description: SAS Client stops responding, when you try to open a folder displayed in the search results.

Subsystem: SAS Client - Search

Platform: Independent

Symptom: If you search for folders using the SAS Client search feature and then try to open the folder displayed in the search results using the Action menu, the SAS Client stops responding.

Workaround: Do not use Open from the Actions menu to open a folder displayed in the search results.

If you open a folder displayed in the search results using Open from the Actions menu and the SAS client stops responding, use your operating system to stop the SAS Client and then restart the SAS Client again.

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: 139028

Description: In the search results the values for the Type of patch policy are displayed as Dynamic or Static.

Subsystem: SAS Client - Search

Platform: Independent

Symptom: In the SAS client, when you search for patch policies, the values for the Type of patch policy in the search results are displayed as Dynamic or Static. The value Dynamic corresponds to Vendor Recommended and the value Static corresponds to User Defined.

Workaround: None.

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.

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

Patch Management

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: 132907

Description: The uninstall patch process failed with an exit code -3, which means that the Agent was unable to find the uninstaller for the selected patch.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: When you tried to uninstall a patch that was installed with Patch Management and the Agent could not find the uninstaller for that patch, the uninstall process failed. (A black check mark in the Installed column in the All Managed Servers preview pane indicates that the patch was installed by Opsware.)

Workaround: Use the Windows Add or Remove Programs tool to uninstall a patch from a server.

Bug ID: 137322

Description: If you created patch policy remediate jobs in Opsware 5.5 and are using Opsware 6, you will not be able to see those jobs in Opsware 6.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: You look in My Jobs in the Opsware Command Center and in Jobs and Sessions in the SAS Client for patch policy remediate jobs you created when you were using Opsware 5.5 and do not see them.

Workaround: None

Bug ID: 138736

Description: Some patches cannot be uninstalled with the SAS Client; however, they can be manually uninstalled.

Platform: Windows

Subsystem: SAS Client - Patch Management for Windows

Symptom: An error occurred when you tried to uninstall this patch from a server.

Workaround: Use the Add or Remove Programs utility on the server to uninstall these types of patches.

Bug ID: 138810

Description: Error in remediating Windows XP Service Pack 2 using Patch install or provisioning Windows XP SP2 due to firewall issues

Platform: Windows XP Service Pack 2 (SP2)

Subsystem: Patch Management/OS Provisioning

Symptom: This issue occurs for Windows XP Service Pack 2 when you either try to install SP2 as a patch policy, or if you attempt to install the operating system using the OS provisioning feature.

If you attempt to install Windows SP2 using a Patch Policy, the Windows XP SP2 binary automatically enables a firewall on the system which prevents the Opsware Agent (as well as other server software) from functioning and communicating with the Opsware core. As a result, the service pack in the patch policy will not be installed on the target server.

If you attempt to provision a server with the Windows XP operating system with SP2, the same problem will occur - the Opsware Agent will not be able to communicate with the Opsware core and the OS will not be installed.

Also, the default Windows XP “Welcome” screen feature can prevent the server from being rebooted, which prevents successful patch installation and OS installation. Thus, this feature needs to be disabled.

Workaround:

For both installing the Windows XP SP2 as a Patch policy and installing this operating system using OS provisioning, you will need to do one of two things:

- Make sure that the Windows firewall option is disabled.

  Or

- Enable the firewall to open the ports necessary for the Opsware Agent to communicate with the Opsware Core.

Regardless of which option you choose, you will also need to do the following:

- Disable the default windows “Wecome Screen”.

Disable Windows XP SP2 Firewall Setting

To disable the Windows XP Service Pack 2 firewall, the following pre-install script should be setup on the WIndows XP SP2 unit record:

```
reg add
HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile
/v
EnableFirewall /t REG_DWORD /d 0
reg add
HKLM\Software\Policies\Microsoft\WindowsFirewall\StandardProfil
e /v
EnableFirewall /t REG_DWORD /d 0
```

Open Ports for Opsware Agent on Windows XP Firewall

To instruct the Windows XP firewall to open the necessary ports for the Opsware Agent, the following post-install script should be setup on the XP SP2 unit record:

```
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\GloballyOpenPorts\List
/v 1001:TCP /t REG_SZ /d 1001:TCP:*:Enabled:OpswareLogbot
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\GloballyOpenPorts\List
/v 1002:TCP /t REG_SZ /d 1002:TCP:*:Enabled:OpswareAgent
reg add
```

```
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\GloballyOpenPorts\List
/v 1002:UDP /t REG_SZ /d 1002:UDP:*:Enabled:OpswareAgent
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\GloballyOpenPorts\List
/v 1023:TCP /t REG_SZ /d 1023:TCP:*:Enabled:OpswareSyncbot
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List
/v 1001:TCP /t REG_SZ /d 1001:TCP:*:Enabled:OpswareLogbot
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List
/v 1002:TCP /t REG_SZ /d 1002:TCP:*:Enabled:OpswareAgent
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List
/v 1002:UDP /t REG_SZ /d 1002:UDP:*:Enabled:OpswareAgent
reg add
HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List
/v 1023:TCP /t REG_SZ /d 1023:TCP:*:Enabled:OpswareSyncbot
```

Disable Window XP SP2 Welcome Screen

To disable the Welcome screen:

1. Open the Control Panel.
2. Select User Accounts.
3. In User Accounts, select the “Change the way users log on or off” option.
4. Uncheck “Use the Welcome screen”.

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

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: 136305

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

Platform: Independent

Subsystem: SAS Reports - User and Security Reports

Symptom: The 'Customer/Facility Permissions and Device Group Permission Overrides' can report take a very long time to run, in some cases, over 30 minutes. When it finishes, the SAS Client freezes and the report results are not scrollable. In some cases, depending upon the amount of data being reports, the SAS Client will hang.

Workaround: None. If you see this error and have questions, please call Opsware support.

Bug ID: 133652

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

Platform: Independent

Subsystem: SAS Client - Reports

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

Workaround: See the information displayed in the Customer column.

Bug ID: 134581

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

Platform: Independent

Subsystem: SAS Client - Reports

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

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

Software Management

Bug ID: 134489

Description: In the Package window, the Files/Scripts tabs on the Packages: Contents view contains no data for RPM and Zip packages.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: When you open the Package window for a RPM or Zip Package, and from the Content view select the Files or Scripts tab, the following exception occurs:

```
SEVERE  ContentElement: Could not load meta data.
java.lang.ClassCastException
```

Workaround: None.

Bug ID: 135068

Description: Cannot assign a software policy at the root level to a user group.

Platform: Independent

Subsystem: AAA (Security), Software Management

Summary: If a software policy is at the root (top) level in the folder hierarchy, it cannot be assigned to a user group because the permissions (and other properties) of the root folder cannot be changed with the SAS Client. (A policy at a lower level is assigned to the user groups that have been specified for the policy's parent folder.)

Workaround: Do not create or put software policies at the root level.

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: 137610

Description: Unable to delete a package in the SAS Client.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client you are unable to delete packages even if the packages are not in use. You are also not able to delete a folder if the folder contains packages.

Workaround: None

Bug ID: 137852

Description: Install Software Policy Template is not enabled when you select multiple software policy templates.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client, if you select multiple software policy templates then in the Actions menu, the option "Install software Policy Template" is not enabled.

Workaround: In the SAS Client, select one software policy template, and then select the option "Install software Policy Template" from the Action menu.

Bug ID: 137989

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: 138146

Description: Unable to delete a folder containing a package which is not in use.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client, when you try to delete a folder containing a package which is not in use you get the following error message:

```
"Unable to delete item"
```

If you try to delete the same folder again, you are able to delete the folder.

Workaround: After you delete the folder the first time, wait for a few seconds and then delete the folder again.

Bug ID: 138696

Description: Server displays as non-compliant when a policy containing packages of multiple platforms is applied.

Subsystem: SAS Client- Software Management

Platform: Independent

Symptom: In the SAS Client, when you remediate a server against a software policy containing packages belonging to multiple platforms of the same platform family and then run a software compliance scan, then the server is always displayed as non-compliant.

Workaround: None.

Bug ID: 138864

Description: In the SAS Web Client, folder search does not display folders to which you are assigned only List permissions.

Subsystem: SAS Web Client - Permissions

Platform: Independent

Symptom: In the SAS Web Client, in the My Profile page you can select the Resource Privileges tab and search for folders to which you have permissions. The search results displays the name of the folder and the permissions for that folder. If you are assigned only "List" permission to a particular folder in Opsware SAS, then the folder does not show up in the search results.

Workaround: None.

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: 138945

Description: The compliance status of a server is not updated when you update a software policy.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: When you perform a software compliance scan, if all the software policies attached to a server are compliant, the server is said to be compliant and is represented by a green icon. If you update a software policy then the compliant status for the server still shows as "Compliant" instead of "Scan Needed".

Workaround: To update the compliance status a status of a server, select Scan Software Compliance from the Action menu to perform a software compliance scan.

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: 139371

Description: Exception is thrown when running the Software Migration Tool with the `-c -f` option.

Platform: Independent

Subsystem: Software Management - Content Migration

Symptom: When you run the Software Migration Tool with the `-c -f` option, you will receive the following exception:

```
[root@purple1 swmgmt]# more swmgmt_migration_error_log
java.rmi.ServerException: RemoteException occurred in server
thread; nested
exception is:
java.rmi.RemoteException: EJB Exception: ; nested exception is:
java.lang.RuntimeException: Could not flush entity updates
```

Workaround: In Opsware SAS 6.0.2, the `-c -f` option is not supported. To perform a full migration, run the Software Migration Tool with the `-f` option.

Bug ID: 139469

Description: Unable to run ISM Controls on a private device group.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: In the SAS Client when you select a private device group, and right-click on the device group, the Run ISM Controls menu option is disabled.

Workaround: Select a member of the private device group and then select run ISM Control menu option.

Bug ID: 139655

Description: Unable to download a Solaris response file using the SAS Client.

Subsystem: SAS Client- Software Management

Platform: Solaris

Symptom: In the SAS Client, downloading (exporting) a Solaris package response file fails with the following error:

Communication with the package repository failed

Workaround: None.

Bug ID: 139713

Description: Importing a RPM package with EUC-KR encoding displays product name of the package with question marks (?).

Subsystem: SAS Client- Software Management

Platform: Solaris

Symptom: In the SAS Client, when you import a RPM package with EUC-KR encoding, the product name of the package appears with question marks(?).

Workaround: None.

Bug ID: 139767

Description: Custom Attributes defined in the source software policy are not copied to the new software policy.

Subsystem: SAS Client- Software Management

Platform: Independent

Symptom: When you copy a software policy to the same folder or a different folder, the custom attributes defined in the source software policy are not copied to the new software policy.

Workaround: None.

Bug ID: 137387

Description: Performing the Software Management data migration causes multimaster conflicts

Platform: Unix

Subsystem: Software Management - Content Migration

Symptom: When running the Software Migration Tool to migrate the data in your Software Tree to software policies in the SAS Client, the data migration causes multimaster conflicts in the Opsware SAS Model Repository.

Workaround: Use the Multimaster Tools in the SAS Web Client to resolve the conflicts. See the Opsware SAS Administration Guide for details on using the Multimaster Tools. Or, if necessary because the Model Repository contains numerous conflicts, run the force_resolver.py script with the –refresh option to resolve the conflicts caused by the data migration. Run the script multiple times if necessary. Contact your Opsware SAS support representative for information about running the force_resolver.py script.

Bug ID: 139298

Description: Application, Service Levels, and Templates not locked after migration

Platform: Independent

Subsystem: Software Management - Content Migration

Symptom: If you run "rollback migration," "complete migration" or "Preview (-m)" before running the actual "full migration," the Software Migration Tool creates the top level folders in the SAS Client in the Software Library; then, when you run the "complete migration," the Software Migration Tool unlocks the Software Tree top-level categories in the SAS Web Client.

Workaround: None. Do not run "rollback" or "complete" migration before running "full" migration.

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.

Visual Application Manager

Bug ID: 139071

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

Platform: Independent

Subsystem: SAS Client - Visual Application Manager

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

Workaround: In the Open window, select both the .vam file and the older topology that you want to open and then double-click that .vam file to open it.

Visual Packager

Bug ID: 139465

Description: Some unreadable Windows objects unable to be packaged and applied to target servers using Visual Packager

Platform: Windows

Subsystem: Visual Packager

Symptom: In some cases, when you attempt to package an unreadable object from a server, you will not be able to package the object and then apply the packaged object to a server, even though the Packaging user interface appears to have packaged the object. For example, some Windows objects such as files, Windows Registry keys, IIS Metabase objects, and so one, might be unreadable due to lack of adequate permissions. When you attempt to package such objects, the Visual Packager user interface will appear to package the objects, but when you apply the package to a target server, the objects will not be applied.

Workaround: None

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: 139620

Description: After switching tabs, Skip and Choose File buttons remain disabled when the first listed package is selected in the table for packages that need to be added to the software repository

Subsystem: SAS Client- Visual Packager

Platform: Independent

Symptom: In the Create Package window, you can select the Contents tab to add packages to the software repository. After selecting the Contents tab, if you select the Details tab and then again select the Contents tab, the buttons Skip and Choose File are disabled in the Create Package window when the first listed package is selected.

Workaround: Select another package in the list, then reselect the first package. If there is only one listed package then close the Create Package window and open a new window to add packages to the software repository.

Bug ID: 139417

Description: Null Pointer exception occurs when creating a package if the OS is deselected.

Subsystem: SAS Client- Visual Packager

Platform: Independent

Symptom: In the SAS Client creating a package when the OS selections has been deselected results in a Null Pointer Exception.

Workaround: Close the Create Package window and open a new window. In the new window create a package without deselecting the OS values.

Chapter 5: Documentation Errata

IN THIS CHAPTER

This chapter contains the following topics:

Updates to the Opsware SAS 6.0.1 Planning and Installation Guide

Solaris 10 Patches Required for Model Repository Install

The Opsware Installer hangs during the installation of the Model Repository. The Oracle alert.log has errors such as the following:

```
MMNL absent for 28552 secs; Foregrounds taking over
Wed Aug  2 12:45:57 2006
MMNL absent for 28853 secs; Foregrounds taking over
Wed Aug  2 12:50:57 2006
MMNL absent for 29151 secs; Foregrounds taking over
```

This bug is specific to Oracle 10.2 and a specific version of Solaris 10 (the T200 hardware and the associated OS patches). Customers should look at Bug 6385446 from Sun Microsystems and apply Patches 118833-18, 119578-24 and 119254-24 as per:

```
http://sunsolve.sun.com/search/document.do?assetkey=1-26-
102289-1
```

System Diagnosis Errors and Additional Database Privileges

If an additional privilege (permission) has been made manually to the database, when Opsware SAS performs a system diagnosis on the Data Access Engine, an error message might be generated. For example, if an additional grant has been made to the `truth.facilities` table, the following error appears:

```
Test Information
Test Name: Model Repository Schema
Description: Verifies that the Data Access Engine's version
of the schema
matches the Model Repository's version.
Component device: Data Access Engine
(spin.blue.qa.opsware.com)
Test Results: The following tables differ between the Data
Access Engine and
the Model Repository:  facilities.
```

To fix this problem, revoke the grant. For example, if you need to revoke a grant on the `truth.facilities` table, log on to the server with the database and enter the following commands:

```
su - oracle
sqlplus "/ as sysdba"
grant create session to truth;
connect truth/<truth passwd>;
revoke select on truth.facilities from spin;
exit
sqlplus "/ as sysdba"
revoke create session from truth;
```

Additional Option Needed for passwd Command on OGFS Server

This problem occurs if the user needs to change a Unix password on the server that runs the OGFS. Because the Opsware PAM module alters /etc/nsswitch.conf, the passwd program needs an additional option to function correctly.

The passwd program would normally be used like this

```
# passwd username
passwd: Changing password for username
passwd: Unsupported nsswitch entry for "passwd:". Use "-r
repository ".
Unexpected failure. Password file/table unchanged.
```

It needs to be used like this:

```
# passwd -r files username
passwd: Changing password for username
New Password:
Re-enter new Password:
passwd: password successfully changed for username
```

Updates to the Opsware SAS 6.0.1 Policy Setter Guide

The followings topics in the Opsware SAS 6.0.1 Policy Setter's Guide are updated with new information:

OS Provisioning – Uploading Build Customization Scripts

In the OS Provisioning feature, uploading build customization scripts into Opsware can be done on one of two ways, depending upon what version of Opsware SAS you are installing and whether or not you are upgrading from a pre-6x version.

- If you are upgrading to Opsware SAS 6.0.1, you should use the upload package functionality in the SAS Web Client or by using the OCLI.
- If you are a new customer installing 6.0.1, you will need to use the OCLI to upload build customitization script. Contact your Opsware Administrator for assistance.

Remediating a Software Policy with Limited User Permissions Note

If you add a package to a software a policy and after the remediation you realize that the policy and the package were not installed – and you receive no error message or warning – it could be due to a permissions issue. The determination of the that get installed on remediation is a combination of user permissions, device customer assignment, and device platform. Refer to the Opsware SAS Administrator's guide for more information on setting Opsware permissions.

Creating a Package

The section "Creating a Package" in the chapter Visual Packager is updated to include the following information.

In Visual Packager, if you create a package from a managed server or audit results with Installed Patches as the selection criteria, and if the Windows patch record does not exist in the patch database, the package is not created.

Packaging Server Setup

The section "Packaging Server Setup" in the chapter Visual Packager is updated to include the following information.

Opsware SAS 6.0.1, Visual Packager only supports packaging servers that have ISM Tool Version 3.1.x installed. When you upgrade from an earlier version of Opsware SAS to Opsware SAS 6.0.1, packaging servers which have ISM Tool 2.0.12 installed are not available in the SAS Client.

Updates to the Opsware SAS 6.0.1 Content Utilities Guide

Content Migration Best Practices for DET

Wait until the migration from 5.x to 6.0.1 completes before importing with DET. Errors occur in the following scenario.

1. Export nodes such as service levels and templates from a 5.x core.
2. Upgrade the core to 6.0.1.
3. Start, but do not complete, the content migration of the core to 6.0.1.
4. Try to import the exported service levels and templates into the 6.0.1 core. These nodes are locked and cannot be imported. During the import an error message (exception) such as the following appears:

   ```
   <class=com.opsware.ejb.session.RoleClassImpl>
   <method=assertLCCertifiedAccess> <message=
   'Cannotmake a parent unlocked when some of its children are
   locked.'>
   ```

For more migration best practices, see the *Opsware® SAS Content Migration Guide*.

Chapter 6: Contacting Opsware, Inc.

IN THIS CHAPTER

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

- Opsware Technical Support
- Opsware Training

Opsware Technical Support

To contact Opsware Technical Support:

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

E-mail: support@opsware.com

For information about Opsware Technical Support:

URL: https://download.opsware.com

Opsware Training

To contact Opsware Training:

E-mail: education@opsware.com

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

For information about Opsware Training:

URL: www.opsware.com/education