Opsware® SAS 7.0 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

Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Opsware Inc. Unpublished Confidential Information. NOT for Redistribution. All Rights Reserved.

Opsware is protected by U.S. Patent Nos. 6,658,426, 6,751,702, 6,816,897, 6,763,361 and patents pending.

Opsware, SAS Web Client, Model Repository, Data Access Engine, Web Services Data Access Engine, Software Repository, Command Engine, Opsware Agent, Model Repository Multimaster Component, and Code Deployment & Rollback are trademarks and service marks of Opsware Inc. All other marks mentioned in this document are the property of their respective owners.

Additional proprietary information about third party and open source materials can be found at http://www.opsware.com/support/sas700tpos.pdf.

Table of Contents

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Chapter 1: What's New in Opsware SAS 7.0

IN THIS CHAPTER

This section contains the following topics:

Opsware Server Automation System (SAS) 7.0 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 SAS7.0 release.

For information regarding new features for the Opsware Application Storage Automation System (ASAS) and the Opsware Operational Management Database (OMDB) clients, please refer to the *Release Notes* for those products.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Audit and Remediation

In the Opsware SAS 7.0 release, there are several new features and enhancements in the Audit and Remediation feature:

- New Audit and Remediation Rules
- Audit and Remediation Rule Enhancements
- "Reflexive" Auditing with Snapshot Specifications
- Improved Audit and Snapshot Results Accessibility
- Archiving Audit and Snapshot Results
- Audit Policies in Folders
- Global Remediation of Audit Results
- Inventory Snapshots

New Audit and Remediation Rules

The following new Audit and Snapshot rules leverage the SAS 7.0 server module architecture for richer and more comprehensive auditing and snapshot taking of servers and server groups:

- Internet Information Services (IIS) Metabase
- Local Security Settings
- .NET Framework Configuration
- Registered Software (patches and packages)
- Runtime State
- Windows Users and Groups
- Unix Users and Groups
- Storage

Audit and Remediation Rule Enhancements

The following Audit and Remediation rules have been enhanced for the Opsware SAS 7.0 release:

- **COM+ Rule Enhancements**: Two new options for COM+ have been added:
  - COM+ rules now capture Access Control Levels (ACLs) for COM+ objects

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

  - You now have the option of comparing only relative filenames instead of the full pathname

- **IIS Metabase Rule Enhancement**: When reviewing the results of the AdminACL or any metabase ACL object, ACLs are displayed with much more detail than before, just as the file system rules show ACLs.
- **File System Rules Enhancements**: File system rules have been enhanced to check all aspects of file ACLs, which are visible in the Audit or Snapshot result. This provides a better view into what is different in an Audit result and provides clearer information to the person who performs remediation.

  Also, for file or directory wildcard settings, you now have the ability to parameterize filenames for Opsware or Custom Attributes. Now, when you create a file rule in an audit or snapshot specification, you can reference environment variables and custom attributes in the file name.
- **Users and Groups Rules Enhancements**: Previously, all users and groups Audit and Snapshot rules were based upon prebuilt TON checks, not upon a specific computer's users and groups. In this release – using the new server module architecture – Audit and Remediation provides the capability to capture all objects on a source server (Windows or UNIX) and use them as the basis for the Audit or Snapshot rule.
- **Registered Software (Packages and Patches) Rule**: You are now able to define rules for an Audit or Snapshot's patches or package object, such as specifying a software patch or package (by name, by date, by vendor, and so on) to determining if it exists on a target.

"Reflexive" Auditing with Snapshot Specifications

This new feature allows you to select a Snapshot Specification as the source of an Audit. This enables you to Audit and see any differences that may occur on a server, comparing a server's ideal configuration against its current configuration over time.

Improved Audit and Snapshot Results Accessibility

You are now able to see relationships between an Audit or Snapshot and its results in a single window. When you select an Audit/Snapshot, you can now automatically see a list of Audit/Snapshot results related to the selected item that expands in a preview pane below the Audit/Snapshot list.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Archiving Audit and Snapshot Results

If you would like to clean up the Audit/Snapshot list, but would not like to delete the Audit/Snapshot altogether, then they have the option of archiving the results related to the selected Audit/Snapshot.

Automatic Removal of Audit and Snapshot Results: You can now schedule Audit and Snapshot results to be automatically removed after a certain date. This feature is especially useful for those recurring Audit and Snapshot jobs that yield copious results.

Using the SAS Web Client, you can schedule audit and snapshot archives to be deleted from the core permanently after a certain period of time.

Audit Policies in Folders

You can now save Audit polices to the Folders inside the SAS Client, allowing for better storage, organization, and accessibility of Audit policies for team members.

Global Remediation of Audit Results

You now have the ability to perform a “mass remediation” of Audit results, by all servers targeted in the Audit, or by all discrepancies discovered in the Audit. This is more efficient and can save a great deal of time when remediation those server configurations that are out of compliance.

Inventory Snapshots

Selecting this option causes SAS to tag the data output of the Snapshot operation as a full manifest or full inventory of the domain area targeted by the server module, and provides richer searching capabilities of the results.

Compliance View

Opsware SAS 7.0 Compliance View for servers and device groups has been greatly enhanced and redesigned for better visibility into the state of compliance of devices in your data center, as well as quick access to remediate non-compliant devices.

This release includes the following new features and enhancements:

- Compliance Rollups for Device Groups
- Redesigned Compliance View for Individual Devices
- Enhanced Device Groups Compliance Threshold Control

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

- Duplex Compliance Test Moved Into Audit Roll Up

Compliance Rollups for Device Groups

In this release, the Compliance View has been greatly redesigned to provide compliance rollup status for device groups, in addition to each individual server. From the device groups list in the SAS Client, you can select one or several device groups and see compliance statuses for all devices in the selected groups (including devices in all sub-groups). From this view, you have access to each compliance category's remediate options for Audit, Software, Patch, App Config.

Redesigned Compliance View for Individual Devices

In this release, an individual server's Device Explorer shows an easy to understand compliance pie chart that represents compliance status for all compliance policies associated with the server. Beneath the pie chart, you can see rollup as well as individual compliance statuses for each category (Audit, Software, Patch, App Config), and access remediate options for each.

In addition, the Device Explorer also gives you access to all policies attached to the server, as well as any archived audits.

Enhanced Device Groups Compliance Threshold Control

The Opsware Administration tool from the Navigation pane now gives much richer control of device group compliance settings in the SAS Client (saved as part of the user who is currently logged in):

- **Show or Hide Device Group Compliance**: Allows you to show or hide dashboard compliance for Device Groups. For example, you might only be interested in viewing compliance for Audit, and so you can hide all other compliance categories so you can see only Audit compliance for selected groups.
- **Member Calculations**: Allows you to choose whether or not to consider devices in sub-groups as part of the compliance status calculation for device group compliance.
- **Server and Device Groups are Considered**: Allows you to specify compliance status roll up to include all members of a device group, including other device groups.
- **Only Server Members are Considered**: Allows you to specify that only server members of a device groups to be used to calculate compliance for selected device groups.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

- **Thresholds**: This new feature allows you to define the threshold levels for determining group compliance levels for all compliance categories.

Duplex Compliance Test Moved Into Audit Roll Up

The Duplex compliance no lives inside the Audit list of tests by selecting Duplex Check from the column selector in the Audit category. Once selected, the it will appear in the Dashboard as its own column.

New Architecture: SAS Core Component Bundling

The release of Opsware SAS 7.0 introduces the concept of Opsware *Core Component Bundling* as a way of distributing Core Components in an Opsware installation. Certain components are *bundled* together and must be installed as a *unit* during a Typical Installation. During a Custom installation, certain components can be broken out of their bundles (such as the Opsware Command Engine, the OS Provisioning Boot Server and Media Server, among others) and installed on separate servers. For more information about SAS Component bundling, see the Opsware SAS Planning and Installation Guide.

Component Bundling provides the following benefits:

- Added simplicity and robustness for multi-server deployments
- Scaling capability: you can install additional Slice Components bundles for horizontal scaling
- Improved High Availability
- Load balancing between slices when multiple instances installed

SAS Client User Interface Enhancements

This release highlights numerous enhancements and improvements in the SAS Client user interface, including the following changes:

- **Device Explorer:** The Device Explorer – the browser that allows you to view details about your servers, network devices. storage assets – has been redesigned to organize information about devices in a more logical manner. Now you can browse basic property information, compliance statuses and attachments, group membership, as well as custom attributes, change history, and more.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

- **Search**: You can now search for ASAS and VAM objects with the SAS Client Search tool.
- **New Library Server Objects**: The SAS Client now includes VAM Business Applications, databases (for ASAS-enabled cores), and well as several new server objects, including Registered Software (patches and patches installed on a server), Windows and Unix Users and Groups, and more.
- **Folders**: You can now save Business Applications and Audit Policies to Folders

Software Management Enhancements

The SAS 7.0 release includes the following Software Management enhancements:

- Install and uninstall software directly on a managed server without using a software policy.
- Import a software application provided by a software vendor and executables into Opsware and deploy that software application on a managed server.
- Manage server objects such as User's and Groups, Registered Software using a software policy and add server objects to the Library.
- Manage software resources such as scripts and server objects using a software policy.
- Specify the installation and uninstallation order among packages, patches, scripts, application configurations, included software policies, and server objects in the software policy.

Script Execution

The SAS 7.0 release allows you to manage the script execution tasks in the SAS Client. The Script Execution feature in the SAS Client enables you to perform the following functions:

- Organize your scripts into folders and define security permissions to control access of their contents across different users and user groups.
- Create or upload scripts in the SAS Client.
- Run scripts across multiple Unix or Windows servers or server groups.
- Execute scripts in the Opsware Global Shell.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

- Schedule one time or recurring script execution jobs.
- Notify the status of the script execution job via email.
- Approve script execution jobs.
- View the script output against multiple servers in a tabular format.
- Export the script execution results.
- Search for scripts and script execution jobs.

Virtualization Director

This release introduces the following functionality for managing VMware virtual machines with the SAS Client:

- Create, modify, and delete
- Execute OS sequence during VM creation
- Power on & off
- Suspend, resume, and restart
- Open console

For more information about Virtualization Director, see the Opsware SAS User's Guide: Server Automation.

Visual Application Manager 7.0

VAM 7.0 is released as part of the Opsware Server Automation System (SAS) 7.0 and provides the following new features:

Storage Visualization

For customers who have ASAS-enabled cores, VAM visualizes logical storage dependencies and physical storage connections (SAN fabric) in your data center and displays how they relate to your business applications – as well as how your servers map to the storage devices they are connected to.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

VAM displays file systems and their relationship to local and remote storage, FC Adapters, FC switches (physical and virtual) connections and ports, disk arrays, NAS filers, LUN mappings, RAID configurations, SAN Fabrics, and more, visible in the VAM maps, panes, tables, and tiers.

Network (LAN & SAN) Enhancements

VAM 7.0 includes the following network visualization enhancements:

- Support for network devices your NAS installation supports
- Visualization of network device and server compliance
- Display of DNS servers in the Properties pane and Server and on the Network Maps (LAN and SAN)
- For network devices (such as firewalls, routers, and switches), you can now view load balancer and ACL configuration information
- For Load Balancers, you can view Server Pool Configuration (in addition to ACLs)

Virtualization Enhancements

VAM 7.0 integrates virtualization relationships into the maps, with the ability to show or hide virtual relationships, where applicable; and, the ability to start stop, pause (VMs only), and restart VMs and Zones

Running Scripts From Inside of VAM

VAM 7.0 supports the ability to run scripts on devices or in the Opsware Global File System (OGFS). You can also run scripts on network devices, given that your user has the proper permissions to perform the action.

Visualization Enhancements

VAM 7.0 includes the following visualization enhancements:

- Display of IPC lines with their associated protocol
- Display of routing table information on a server's Properties pane
- Display of Weblogic and Microsoft IIS properties information and in the VAM maps

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Emailing Contacts

In VAM 7.0, you can create email contacts and associate them with business applications – and send emails to the contacts on the list.

New – Infrastructure Pane

The new Infrastructure pane provides rich detailed information about devices, file systems, compliance policies, network interfaces, and more

Snapshot Enhancements

You now have the ability to schedule VAM Snapshots to run on demand or on a recurring basis. Also, snapshot comparison has been improved for an enhanced ease of use

Adding Devices and Sharing Components

- Ability to add new devices to an existing business application
- Sharing of VAM objects and VAM through URLs using drag and drop into emails or chat windows, or through embedding VAM launch URLs in web pages.

Other VAM Enhancements

- Increased OS platform support
- Improved filtering (searching)
- Easier business application signature Properties editing, including extended application signature discovery using environment variables
- New VAM discovery settings to determine remote server dependencies
- Ability to export tables to CSV

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Chapter 2: Platform and Environment Support for 7.0

IN THIS CHAPTER

This chapter contains the following topics:

- Supported Operating Systems for SAS 7.0
- Supported Core Operating Systems for 7.0
- Types of Opsware SAS Installations
- Operating System Deprecation and End of Support
- Documentation for Opsware SAS 7.0

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Supported Operating Systems for SAS 7.0

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	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

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

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

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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Opsware SAS Client

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

Table 2-2: SAS Client Supported Operating Systems

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

Supported Core Operating Systems for 7.0

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

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

Table 2-3: Opsware Core Supported Operating Systems

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

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

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

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

Table 2-4: Opsware Satellite Supported Operating Systems

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

Types of Opsware SAS Installations

There are three basic types of Opsware SAS installations: First Core (Single Core), Multimaster Mesh, and Satellite Core.

- **First Core or Single Core** (formerly Standalone Core): A Single Core typically provides management capabilities for servers in a single facility.
- **Multimaster Mesh**: A *Multimaster Mesh* is a set of two or more Opsware Cores that communicate through Opsware Management Gateways and can perform real-time synchronization of the data about their Managed Servers contained in their respective Model Repositories over the network.
- **Satellite**: Satellite installations are appropriate for smaller, remote sites that may not have the installed infrastructure for a full Opsware core installation.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

For more information, see the *Opsware® SAS Planning and Installation Guide* for more information.

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 7.0:

- 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 7.0:

- 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.)

Documentation for Opsware SAS 7.0

This release comes with the following documentation:

- *Opsware SAS 7.0 Release Notes*
- *Opsware SAS 7.0 Quick Reference: Pre-Installation Requirements*

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

- *Opsware SAS 7.0 Planning and Installation Guide*
- *Opsware SAS 7.0 Policy Setter's Guide*
- *Opsware SAS 7.0 Administration Guide*
- *Opsware SAS 7.0 User's Guide: Server Automation*
- *Opsware SAS 7.0 User's Guide: Application Automation*
- *Opsware SAS 7.0 Oracle Setup for the Model Repository*
- *Opsware SAS 7.0 Content Utilities Guide*
- *Opsware SAS 7.0 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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Chapter 3: Known Problems, Restrictions, and Workarounds in Opsware SAS 7.0

IN THIS CHAPTER

This chapter describes workarounds for known problems in Opsware SAS 7.0. These descriptions are arranged by the following features:

- Agent Installer
- Application Configuration
- Audit and Remediation
- DCML Exchange Tool (DET)
- Global Shell
- Jobs and Sessions
- Operating System Provisioning
- Opsware Agent
- Opsware Installer
- Opsware SAS Client
- Opsware SAS Web Client
- Patch Management for Windows
- Patch Management for Unix
- PowerShell
- SAS Client Reports
- Script Execution
- Software Management
- Virtualization
- Visual Application Manager (VAM)

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

For information regarding open issues for the Opsware Application Storage Automation System (ASAS) and the Opsware Operational Management Database (OMDB) clients, please refer to the *Release Notes* for those products.

Agent Installer

Bug ID: 155270 (See also 154714)

Description: Install fails when reinstalling Opsware SAS 6.5.1.3 to a server that has an Opsware SAS 6.5.1.2 agent installed.

Platform: Independent

Subsystem: Agent Installer

Symptom: When installing Opsware 6.5.1.3 to a server that already has an Opsware SAS 6.5.1.2 agent installed, the following error occurs:

```
[INFO] Stopping Opsware agent.

[INFO] Removing non-legacy agent files.

[INFO] Installing Opsware agent into 'C:\Program
Files\Opsware\agent'.

[INFO] Agent unpack deferred to InstallN() for atomic delivery.

[ERROR] Opsware agent installation failed.

[ERROR] Unable to open service : 'opswareagent' : Error : (1060)
: 'The specified service does not exist as an installed
service.'.

[ERROR] Opsware agent could not be started.

[WARN] Unable to remove directory
'C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~1804-1.WRK' : Error : (32)
: 'The process cannot access the file because it is being used
by another process.
```

Workaround: Uninstall the Opsware SAS 6.5.1.2 agent then install the Opsware SAS 6.5.1.3 agent.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Bug ID: 139042

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

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rule

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

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

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

Bug ID: 158946

Description: WebLogic Application Configuration post-install script may fail to restart WebLogic without reporting errors.

Platform: Windows or Unix

Subsystem: Application Configuration Engine - Post Install Script

Symptom: When you push a Weblogic Application Configuration which includes an AppConfig post-script, in some cases WebLogic is not restarted, and no error is reported. In the current implementation, the script starts WebLogic as a background task, instead of waiting for the push to complete.

Workaround: Manually Restart WebLogic

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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 158909

Description: Running audit for user and group or Registered Software (packages and patches) sometimes fails with LegacyException error

Platform: Any

Subsystem: Audit and Remediation

Symptom: Sometimes running an audit for Users and Groups or Registered software will fail due to errors with the Opsware Global File System and the TTGL utility, visible as a LegacyException.

Workaround: Re-run the Audit.

Bug ID: 160047

Description: Snapshots and audits sometimes fail with rules using Unicode characters

Platform: Any

Subsystem: Audit and Remediation - Audits and Snapshots Rules

Symptom: An audit or snapshots could fail if a server module-based rule (for example, User's and Groups, or Registered Software) contains a name with Unicode characters. For example, if you created a user or group with the name that contains Chinese/Japanese/Korean characters, and then you created a snapshot or audit and include that user by

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

specifying its name (or browse and pick its name). When you run the audit or snapshot, the audit or snapshot would be unable to find that user and the results would return empty.

Workaround: Try using a wildcard search string in the rule rather than the specific Unicode character.

Bug ID: 160361

Description: Auditing AppConfig in an audit for large, complex files not producing differences

Platform: Any

Subsystem: Audit and Remediation - Application Configuration Rules

Symptom: In some cases, if you attempt to audit more than one complex configuration files in an Application Configuration rule, the process will take a long time and in some cases, eventually time out. Performing this action on a slow core might also affect this issue. For example, if you tried to audit two very large, deeply nested XM files in an Application Configuration rule, and the core you attempted to perform this on was running on slow servers, the process could timeout and not produce differenced results.

Workaround: None. However, this process might be improved if you upgrade the server that the Spoke is running on.

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

Bug ID: 159641

Description: DET Import Media (cbt import) error when importing OS Sequences with build customization scripts.

Platform: Any

Subsystem: DET Import

Symptom: When performing an import media with the DET import media tool (cbt), if the content being imported contains OS Sequences with build customization scripts, it can cause the entire import to fail at the point at which the import process encounters the OS Sequences that contain build customization scripts.

Workaround: In this case, it is best to add the OS Sequences with build customization scripts manually, and then run the import again but with the "-p skip" option enabled.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.”

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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
```

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

```
/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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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()`.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 145833

Description: Some antivirus programs on the Opsware core servers can prevent various Opsware features such as OGFS, and ODAD from functioning.

Platform: Independent

Subsystem: OGFS

Symptom: Antivirus programs like Sophos antivirus installed on the Opsware core servers are not compatible with OGFS. As a result they prevent Opsware features such as OGFS, ODAD, and Server Explorer from functioning.

Workaround: When you run the OGFS on a core server, disable the antivirus program or configure the antivirus program to ignore the following path:

/var/opt/opsware/ogfs/mnt/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
```

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

```
/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
```

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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
```

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

Workaround: None

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: 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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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:
```

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

```
\\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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Opsware Agent

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: 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 Command Center Web Client (SAS Web Client)

Bug ID: 154691

Description: After restarting the OCC, you must login twice to log in to the OCC Web Client

Platform: Independent

Subsystem: OCC Web Client

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Symptom: Due to a known issue with JBoss/Tomcat, you must log in twice to the OCC Web Client after restarting the OCC. The first time you provide your username and password and select Agree on the User Acceptance screen, although you have been authenticated, you will not be logged into the SAS Web Client. When you log in again, you will be logged into the client normally.

Workaround: None

Bug ID: 160041, 160056

Description: Exporting a large report to .html or Excel can fail and cause the SAS Web to run out of memory

Platform: Any

Subsystem: SAS Web Client - Reporting

Symptom: When running a large report, for example, running a report to display all server permissions where the results would exceed 5000 rows, and if you attempt to export that report to .htm lor .xls, the operation will fail and potentially cause the SAS Web Client to run out of memory.

Workaround: Export the report to .pdf.

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:

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

```
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: 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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

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

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 158212

Description: Actual Windows server's Local Security Settings - Security Options not matching view shown in server's Device Explorer.

Platform: Windows

Subsystem: SAS Client Device Explorer - Inventory Local Security Settings - Security Options

Symptom: In some cases, when you browse a Windows server's Local Security Settings - Security Options in the Device Explorer, not all of the local security settings will display.

Workaround: None

Bug ID: 159906

Description: An error or hang occurs when attempting to log in to the SAS Client.

Platform: Independent

Subsystem: SAS Client/Oracle

Symptom: When attempting to log in to the SAS Client, an error occurs or log in hangs.

The following error may appear in Oracle's `alert.log` file:

```
<datestamp>
```

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

```
Errors in file /u01/app/oracle/admin/truth/udump/truth_ora_
0000.trc:

ORA-00600: internal error code, arguments: [kkslgbv0], [], [],
[], [], [], [], []
```

This error occurs due to Oracle Bug 5155885. You can find more information about this bug at *http:*I*metalink.oracle.com*.

Workaround: Restart Oracle.

Bug ID: 154416

Description: Unable to add registry key HKEY_CURRENT_USER to the Library

Platform: Windows

`Subsystem`: Device Explorer

Symptom: In the Device Explorer when you select the Windows registry key HKEY_CURRENT_USER and then select Add to Library from the Actions menu, then you get the following error:

"Certain content cannot be captured...".

Workaround: None. Opsware does not support adding registry key HKEY_CURRENT_USER to the Library.

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
```

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

```
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

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Bug ID: 148022

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

Platform: Independent

Subsystem: SAS Web 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.

Bug ID: 159229

Description: Random user actions sometimes cause HTTP Status 500 in the SAS Web Client

Platform: Any

Subsystem: SAS Web Client

Symptom: In some cases while performing basic user actions, the SAS Web Client produces an HTTP Status 500 error page. You will also see a ClassCircularException in the error page.

Workaround: Restart the OCC server. To do this, log on to the OCC host server as root and run the following command:

```
/etc/init.d/opsware-sas restart occ.server
```

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Workaround: None

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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

PowerShell

Bug ID: 154417

Description: A PowerShell script which does not exit with an explicit status may result in incorrect script completion status when the script is run using the SAS Client.

Platform: Windows

Subsystem: PowerShell

Symptom: If an error condition or caught exception arises during execution of a PowerShell script, and the PowerShell script exits without explicitly setting an exit status, the exit status will be zero (a caught exception will set the exit status to 1). When such a script is run interactively in the PowerShell interpreter, the user may see an error message or some other indication of an exception, but the exit status will be set to zero unless explicitly set to non-zero by the script developer. Now when the same script is executed by SAS on a managed server, the success or failure of the script execution is based solely on the exit status from the script. Thus, it can appear that the script was successful even though it failed to perform some action, because the exit status from the script is zero. In order to get a failure or exception condition to filter correctly from the script running on the managed server through SAS to the SAS Client, where it can be seen by an operator, the script must be modified to exit with non-zero status when the exception or error condition arises.

Workaround: To always exit a script with the correct exit code, you should use the 'exit' PowerShell statement, for example

```
$file = "C:\file.txt"

if(( test-path( $file ) ) -eq $True )

{ write-host "Found file"}

else { write-host "File not found"; exit 1 }
```

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Bug ID: 158784

Description: profile.ps1 is created for Default user when Opsware SAS PowerShell Connector MSI is installed from the SAS Client.

Platform: Windows

Subsystem: PowerShell

Symptom: If you are logged into a server or workstation as user Administrator, and you manually install the Opsware SAS PowerShell Connector MSI package, the install will create/update a profile.ps1 script at this location:

```
C:\Documents and Settings\Administrator\My
Documents\WindowsPowerShell\profile.ps1
```

However if you use the SAS Client to install the MSI package on a managed server, the profile.ps1 will be created here:

```
C:\Documents and Settings\Default User\My
Documents\WindowsPowerShell\profile.ps1
```

That's because the install operation is performed in the context of Local System, and not Administrator or some other user account.

Workaround: None.

Bug ID: 153788

Description: SAS Jobs listed in the SAS Client does not match the Jobs listed when running the command Get-SASJob in the PowerShell command line interface.

Platform: Windows

Subsystem: PowerShell

Symptom: When you run the Get-SASJob cmdlet, you may find that the number of returned jobs differs from the number visible in the SAS Client. This happens because the SAS Client silently filters out certain jobs that the Get-SASJob cmdlet does not filter out. For example, jobs which are in state DELETED are not shown in the SAS Client, but are returned by the Get-SASJob cmdlet.

Workaround: None.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Bug ID: 159364

Description: Running an Audit and Remediation containing a PowerShell script on a managed server on which PowerShell is not installed leads to an uncaught exception and failure of the remediation..

Platform: Windows

Subsystem: PowerShell

Symptom: If PowerShell is not installed on a managed server and you run an audit remediation containing a PowerShell script on that managed server, then the remediation will fail with an uncaught exception. The exception text will contain “PowerShell is not installed on this server”, along with a traceback.

Workaround: Install PowerShell on the managed server.

Bug ID: 158487

Description: Unable to install Opsware SAS PowerShell Connector MSI Package on Windows Vista.

Platform: Windows

Subsystem: PowerShell

Symptom: When you install a Opsware SAS PowerShell Connector MSI Package on Windows Vista as an Administrator User, the install fails with error code 2869.

Workaround:

1. Create a batch file with the following command:

   ```
   msiexec /i "path-to-package.msi"
   ```

2. Save the file
3. Right-click it and then select “Run as Administrator”

SAS Client Reports

Bug ID: 133350

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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 160041, 160056

Description: Exporting a large report to .html or Excel can fail and cause the SAS Web to run out of memory

Platform: Any

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Subsystem: Reporting – SAS Web Client

Symptom: When running a large report, for example, running a report to display all server permissions where the results would exceed 5000 rows, and if you attempt to export that report to .htm lor .xls, the operation will fail and potentially cause the SAS Web Client to run out of memory.

Workaround: Export the report to .pdf.

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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: 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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

Bug ID: 159227

Description: Selecting too many individual parameters on a multi-select list in a report can cause a report to not run. (For OMDB-enabled cores only.)

Platform: Independent

Subsystem: Reports – OMDB

Symptom: Selecting a large number of values in the Select Values window of a report can cause the report to not run.

Workaround: Choose any of the following options:

- Use alternative operators to Equals. For example, selecting Contains and leaving the field blank returns the same results as selecting Equals and selecting all the values in the Select Values window.
- Select fewer values.
- If using Equals, select the default [Any value].

Script Execution

Bug ID: 155135

Description: Deleting a script referenced by an OS Sequence leads to null pointer exception.

Platform: Independent

Subsystem: Script Execution

Symptom: In the SAS Client if you perform the following actions:

1. Add a script to the Run OS Sequence Remediate Policies view's Pre/Post Remediate script.
2. Delete the script referenced by the OS Sequence from the Library in the SAS Client

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

3 Reopen the OS Sequence

then the following null pointer exception is thrown:

```
SEVERE Trying to setup refs for ReconcileTask
java.lang.NullPointerException
```

Workaround: In the SAS Client do not delete a script if it is referenced by an OS Sequence.

Bug ID: 157422

Description: Setting the Version of a script as current, may lead to an * being displayed in the title bar of the script window.

Platform: Independent

Subsystem: Script Execution

Symptom: In the SAS Client when you perform the following actions:

1 In the script window, select a Version History from the navigation pane

2 From the Content pane, select a script

3 From the File menu select Set as Current Version

4 In the view drop-down list, select Properties.

then the version of the script is set to current and in the Script window title bar an * is displayed. This behavior is observed only intermittently. If you Save the script, then a new version of the script is created.

Workaround: None.

Bug ID: 158307

Description: Error message does not indicate if a script failed due to timeout.

Platform: Independent

Subsystem: Script Execution

Symptom: In the SAS Client if you run a script, and if the script failed due to timeout, then the error message does not indicate the reason for script failure.

Workaround: None.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Bug ID: 159213

Description: Policy Usage for a saved server script is not visible if you have only Execute permission on the folder.

Platform: Independent

Subsystem: Script Execution

Symptom: If you open a saved server script in the SAS Client, in the script window you are unable to view the Policy Usage for the saved script. This behavior is only observed if you have the following permissions:

Manage Server Scripts: Read

Folder Permission: Execute objects in Folder.

Workaround: None.

Bug ID: 159878

Description: In the File menu, the Save option is not disabled after you save the script.

Platform: Independent

Subsystem: Script Execution

Symptom: In the SAS Client, when you perform the following actions:

1. Open a script and any make changes to the script to create a new version of the script.
2. Save the script.
3. Do not close the script window.
4. Select the file menu.

then in the File menu, Save and Revert actions are enabled. If you select Save, then a new version of the script is created.

Workaround:

1. In the Script window create a new version of the script.
2. Save the script.
3. Close the script window.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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: 146298

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

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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: 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: 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.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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 an .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 SAS 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.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

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

Bug ID: 153585

Description: During software uninstallation/installation, when the server has to reboot, the Job Status continues to displayed as “uninstalling”/”installing” until the reboot has been completed.

Platform: Independent

Subsystem: Software Management

Symptom: In the SAS Client when you uninstall or install software using the Uninstall or Install Software task window and in the Options step, you select the reboot option “Hold all server reboots until all actions are complete”, then in the Job Status window, the uninstall or install software action is displayed as uninstalling or installing and the reboot action is displayed as pending until the software action and server reboot is completed.

Bug ID: 159282

Description: Post-Install or Post-Uninstall script is not executed during software installation or uninstallation if a failure occurs.

Platform: Independent

Subsystem: Software Management

Symptom: In the SAS Client when you install or uninstall software, the Post- Install or Post-Uninstall script is not executed if a failure occurs, even when you select the option “Continue if an error occurs”.

Workaround: None.

Virtualization

Bug ID: 143998

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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Platform: Independent

Subsystem: Virtualization - Refresh for Zone Changes

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

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

Bug ID: 160064

Description: A newly provisioned solaris 10x86 VM is shown as an unmanaged VM.

Platform: Solaris

Subsystem: Virtualization Director

Symptoms: Run Create VM with OS provisioning for a Solaris 10x86 VM. In **Servers ➤ Virtual Servers**, the VM is shown as an unmanaged VM. Its Hostname is blank, and its Virtual Machine Name is that of the host ESX 3 server.

Workaround: None

Bug ID: 160078

Description: A Java exception occurs in a ESX 3 Virtualization view

Platform: Independent

Subsystem: Virtualization Director

Symptoms: Select **Servers ➤ Virtual Servers**, Virtualization view. Selecting an ESX server results in the exception `java.lang.IndexOutOfBoundsException: Index: 1, Size: 1`. The Details pane is blank (i.e. the list of VMs is not displayed).

Workaround: None

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Visual Application Manager (VAM)

Bug ID 159767

Description: VAM Business Application components turn red when a Business Application is saves as a .vat file, without feedback that scan data is lost during export.

Platform: Any

Subsystem: Visual Application Manager – Save Business Application

Symptom: When you save a .vat file (a VAM Template), by design all scan information will be lost, including the servers and devices and their relationships. Business Application definitions and all the components inside of them remain after an export, but turn red to indicate that relationships between live processes and connections have been lost.

Workaround: None.VAM templates do not contain scan information. If you want to retain scan information, save as a .vam file (a VAM Archive) or Business Application.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Chapter 4: Documentation Errata

IN THIS CHAPTER

This chapter contains the following topics:

Update to the Opsware SAS Planning and Installation Guide, Chapter 3: Pre-Installation Requirements

The following note should be added under the heading: “SAS Core Server Package Requirements”, “Linux Package Requirements”:

If you need to remove the Samba package, samba has dependencies on `control_center` and `gnome-libs` under Red Hat AS 4 (x64). These two packages are required by the Opsware-supplied Oracle database so you must use the `--nodeps` argument to remove Samba without considering dependencies.

Update to the Opsware SAS Quick Reference re-Installation Requirements for Opsware SAS 7.0

The following paragraphs were omitted under the heading “SAS Core Server Package Requirements”:

To verify that the samba package, for example, is installed, enter the following command:

```
rpm -qa | grep samba
```

You can obtain the latest versions of these packages from the Red Hat errata web site.

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

To remove packages, enter the following command:

```
rpm -e package_name
```

Some packages in this list may be depended on by other packages that are installed on your system. For example, the default Red Hat installation includes `mod_python` and `mod_perl` that depend on `httpd` being installed. In order to remove packages that fulfill dependencies, you must simultaneously remove the packages that create the dependencies. In this example, you would need to enter the following command:

```
rpm -e httpd mod_python mod_perl
```

If `rpm` identifies an additional dependency, it will note which packages have dependencies on the components to be removed and fail. These packages must be added to the uninstall command line. If the chain of dependencies cannot be suitably resolved, enter the `rpm -e --nodeps` command to remove the desired packages without considering dependencies.

Update to the User's Guide: Server Automation, Appendix A: Opsware Agent Utilities

Under the heading “Installing an Opsware Agent by using the Agent Installer CLI”, Step 3 specifies that you must download the agent install package from the library in the SAS client (Java GUI). This is incorrect because the packages are not viewable via the SAS Client.

You must do a command-line download of the agent installer from `/var/opt/opsware/agent_installers` in the core.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

Chapter 5: 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

Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.

 Opsware Inc. Confidential Information: Not for Redistribution. Copyright © 2000-2008 Opsware Inc. All Rights Reserved.