Opsware® SAS 6.0

Release Notes

Version 2.0

Date August 16, 2006

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.

T + 1 408.745.1300 F +1 408.745.1383 www.opsware.com

Opsware SAS Version 6

Table of Contents

Introduction to Opsware SAS 6

Opsware Server Automation System (SAS) 6 provides the features described in the following tables.

Automated Discovery

Capability	Features
Infrastructure Discovery Auto-discovery of servers on the network. Ensures visibility of all servers in the IT environment.	• Initiate network scans for servers from a local host or from a remote host to gain access to all servers regardless of network location. • Based on network scan, Opsware reports on detected OS and available communication mechanism. • Use available communication mechanism to deploy agents and bring servers under Opsware Management.
Server and Application Discovery Auto-discovery of server hardware and software information. Maintains records of this information to provide users up-to-date, contextual knowledge about the environment.	• Populates Opsware data model with automatically discovered hardware information, such as manufacturer, serial number, CPU model, and storage capacity. • Detects and tracks installed software, patches, packages, and configurations. • Automatically updates Opsware data model as configurations change or new software is installed.

Application Dependency Mapping

Capability	Features
Visual Application Manager Interactive application dependency mapping with integrated change automation for servers, software, network devices and applications.	• Quickly discover and map dependencies for the entire application environment. • Map network devices, servers, software, and business application dependencies. • Leverage Opsware Network Automation System for deep discovery of network devices. • Intelligently filter and group information to allow in-depth views of the data center infrastructure and applications. • Targeted views with server, network and logical application options • Easily extensible application signature library for custom application discovery. • Take change and configuration management action from the visual map.
Application-level Visibility View and access servers and network device infrastructure supporting an application. Understand application-level dependencies for troubleshooting.	• Identify device groups that include both server and network infrastructure. • Visualize application dependencies in multiple different views including server, network and logical application view. • Automate discovery of common server and network issues such as duplex mismatch. • Facilitate troubleshooting with an integrated event history for both servers and network devices.

	• Allow login to network devices using the Opsware Global Shell. • Grant granular administrator access permissions around server and network visibility.

Change and Configuration Management

Capability	Features
OS Provisioning Provision operating system baselines onto bare metal servers quickly, consistently, and with minimal manual intervention. Ensures consistent and secure server baselines that can be easily updated, patched, and refreshed to meet corporate standards.	• Bare-metal provisioning of Sun Solaris, Microsoft Windows, Red Hat, and SUSE Linux. • Supports flexible network-based, floppy-based, or CD-based provisioning. • Provisions a wide range of hardware models and VMware Virtual Machines. • Supports standard packaging formats. • Manages and builds complete “best practices” server operating baselines. • Leverages pre-defined patch policies and software policies. • Integration with full range of Server Automation for complete software stack management. • Automatically configures network settings. • Supports scheduling. • Supports re-provisioning. • Automatic replication of operating system builds across multiple facilities (when used with

	Multimaster). • Delivers a secure, task-based user interface.
Patch Management Quickly and accurately identify and patch a large number of servers. Integrated with Compliance Dashboard for at-a-glance compliance with patch policies.	• Precisely identify target servers that require patches. • Automatically detects patches installed on Windows, Linux, Solaris, AIX, and HP-UX servers. • Supports native patching formats. • Apply patches across any heterogeneous environment, including Windows, Linux, Solaris, AIX, and HP-UX servers. • Enables creation and enforcement of patch policies. • Scans Windows servers and automatically compare patch levels against Microsoft's published patch list. • Supports scheduling patch deployments for a later date and time. • Supports patch rollback. • Tailors patch deployment with special scripts or automated reboot. • Audit and report on patch compliance.
Software Management Enable distributed IT teams to collaborate for rapid install, configuration, and removal of applications across many servers, simultaneously. Ensures quality and consistency by leveraging common builds and closely tracking what is deployed on each server. Integrated with the Dashboard for at-a-glance status	• Automates provisioning of software across Solaris, Linux, Windows, AIX, and HP-UX servers. • Centralized software repository that is automatically replicated between data centers (when used in conjunction with Multimaster). • Supports 20+ native packaging technologies for

of software policy compliance.	each operating system, such as MSI, ZIP, and RPM. • Software policy definition combines software content with configuration best practices. • Up-to-date list of what software is currently installed on a server as well as a list of what software should be installed on a server according to policies. • Customize folders to match organizational hierarchy with permission boundaries to protect content across user groups. • Preview what software to install, remove, or leave as-is based on Opsware SAS' knowledge of what software is already installed on a server and the requested operation. • Unified audit trail captures the who, what, when, and where of software provisioning. • Supports scheduling provisioning for a later time and date. • Ability to tailor software provisioning with pre- and post-installation instructions • Ability to perform multi-instance software provisioning. • Easy-to-use wizards automate and guide users through the provisioning process.
Application Control and Configuration Management Create and enforce policy-based management of application configurations objects. Enables administrators to streamline application configuration	• Enables management of file and object-based configurations. • Captures and enforces best practice configuration defaults. • Enables editing of configuration values for

management.	individual servers or server groups in an easy-to-use template. • Visually preview changes between expected and actual state. • Perform necessary steps to enact the changes from Opsware, including pre-install and post-install operations. • Call application controls, such as start, stop, and reconfigure, directly from Opsware SAS without logging onto servers.
Code Deployment and Rollback Distribute and roll back code, content and configurations to multiple servers of different operating systems, simultaneously. Simplifies the handoff from development to operations.	• Seamlessly push code from staging or development environments to production environments. • Synchronize code and content across multiple devices and locations. • Automatically roll back to the previous version of code or content. • Sequence multiple, complex deployment steps into repeatable workflows. • Manage changes across heterogeneous platforms.
Configuration Tracking Track, backup, and recover critical software and system configuration information across Unix and Windows servers located in one or more data centers. Enables administrators to define policy-based configuration tracking.	• Detects manual changes and automatically creates change histories of server configurations and automatically sends email alerts when configuration changes are detected. • Roll back configurations to any previous working state. • Back up configurations at any time.

	• View server configuration audit trails, showing all changes across specified machines. • Supports one-click download of any version of configuration history.
Script Execution Simultaneously and securely share and run ad-hoc or custom scripts across multiple servers and then collect, collate, view and download the results.	• Cross-platform support, including the ability to execute Unix and Linux shell scripts or Windows Visual Basic scripts and batch files. • Mass execution of ad-hoc or saved scripts using GUI or CLI across managed servers. • Private and shared script management. • Role-based access control system to manage who can execute scripts on which servers. • Ability to store and look up values in the Opsware Data Model to customize scripts and execution. • Execute scripts according to user permissions. • Supports scheduling of scripts to execute at a later time and date. • Ability to view the output of a single server or consolidated output for all servers. • Comprehensive audit trail showing the who, what, when, and where for each script execution session.

Audit and Compliance

Capability	Features
Server Audit	• Create audit baseline from live server, template,

Compare servers and synchronize files and directories across servers. Enables rapid troubleshooting and compliance management.	historical server state audit, user-defined values or the results of a script. • Leverage built-in industry best practices, such as CIS Windows 2003 policies, as policy checks. • Run audits on an ad-hoc basis or schedule audits to run on a regular basis. • Save audits for repeated use to test compliance. • Run audits against individual servers or dynamic server groups. • Visually preview file or configuration differences.
Server Remediation Remediate server audit results by creating an installable package of differences.	• Create an installable package to synchronize a server with the baseline. • Select multiple objects or files from a local source or the Opsware data repository. • Save packages in the Opsware data repository for future usage. • Remediate against the results of a script.
Dashboard At-a-glance view of compliance against corporate policies. User configurable and easily extended to include custom policies.	• Roll-up compliance status across multiple policies and groups of servers. • View compliance status on servers against patch, software, and application configuration policies, duplex settings, and custom audit checks. • Drill down on individual checks to view detailed compliance gaps. • Links enable remediation of compliance gaps. • Easily extend the Dashboard to run new checks and views.

	• Export and email results.

Reporting

Capability	Features
Reporting View dynamic, real-time reports into the hardware, software, patches, and operations activities in complex, heterogeneous data centers.	• Comprehensive hardware, software, and operations activity visibility across all locations. Includes all Windows, Linux, Solaris, AIX, and HP-UX servers. • Out-of-the-box compliance reports for common regulations, such as Sarbanes-Oxley. • Customizable compliance reports. • Change history reporting across all servers and software. • View data by server business attributes. • Comprehensive patch reporting across all platforms. • Ad-hoc query capability with up-to-the-moment data accuracy. • Interactive color graphs provide high level data with drill-down capability. • Export to different formats, including Microsoft Word or Excel, or Rich Text Format. • Direct access to database views for easy integration with preferred corporate reporting tools.

Multi- or Remote Data Center Operations

Capability	Features
Multi-Data Center Operations Build and manage servers located in any data center from a single console. Ensures that all operational benefits of Opsware SAS are realized across all data center locations.	• Provides a crucial part of an organization's overall business continuity, or disaster recovery plan by enabling the rebuilding of any server in any environment. • Single web-based interface provides visibility and control over entire global environment. • Real-time, secure replication of critical server and software information to all data centers. • Set global or enterprise-wide policies to be enacted across the entire environment. • Secure, on-demand replication of software packages. • Scheduled backup of all software packages to one of more data centers. • True Multimaster replication between cores. • Scales to support over 1,000s of servers across dozens of data centers.
Automate Management of Servers n Remote Offices Enables IT organizations to extend the benefits of Opsware server and application lifecycle automation with data center quality of service to servers located in remote facilities.	• Complete server and application lifecycle automation for servers in remote facilities via Opsware Satellite. • Allows administrators to specify the amount of network bandwidth for software distribution. • Supports local software caching and updates to

	software cache over the network. • Initiate communications from either Satellite or Opsware core to meet network needs. • Enables management of remote servers by automatically reconciling overlapping IP addresses. • Automatically resumes interrupted downloads. • Update software cache either online or offline. • Supports dynamic re-routing around failed links for redundancy. • Certificate-based authentication for a robust and secure infrastructure. • Unified display of remote servers and data center servers in the user interface.

Productivity Tools

Capability	Features
Secure Remote Terminal Direct access to servers using Opsware's secure communication channel.	• Enables administrators to open a terminal connection to any server in any location. • Allows administrators to use their favorite shell for Linux and Unix and Remote Desktop Connection for Windows. • Automatically records all commands and responses for shell sessions in an audit log.
Global Shell Manage remote systems from a command line	• Supports all common shell and scripting languages.

interface. Enables administrators to perform tasks across multiple servers with efficiency and security.	• Enables execution of multi-server operations. • Allows administrators to access the Opsware data model and individual server file systems to target actions for faster troubleshooting. • Enforces Opsware access control permissions. • Automatically records all commands, responses, and session information in an audit log.
Server Explorer Browse and edit any server in any location from Opsware.	• Allows administrators to browse any managed server including the file system, registry, meta-data, server history, compliance results, and network layer 2 and VLAN information. • Supports drag and drop of files between servers or between a local desktop and servers. • Automatically records all actions taken by administrators in a digitally signed audit log.

Platform and Environmental Support

Supported Operating Systems

The following tables identify the supported operating systems for Opsware Agents, the Opsware Command Center, and the SAS Client.

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

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 11i v2	PA-RISC PA-RISC PA-RISC PA-RISC and Itanium
Sun Solaris	Solaris 6 Solaris 7 Solaris 8 Solaris 9 Solaris 10	Sun SPARC Sun SPARC Sun SPARC Sun SPARC Sun SPARC, 64 bit x86 and Niagara
Fujitsu Solaris	Solaris 8 Solaris 9 Solaris 10	Fujitsu SPARC Fujitsu SPARC Fujitsu SPARC

Supported Operating Systems for Opsware Agent	Versions	Architecture
Windows	Windows NT 4.0 Windows 2000 Server Family Windows Server 2003 Windows Server 2003 x64 Windows XP Professional	32 bit x86 32 bit x86 32 bit x86 64 bit x86 64 bit x86
Red Hat Linux	Red Hat Linux 7.3 Red Hat Linux 8.0 Red Hat Enterprise Linux 2.1 AS Red Hat Enterprise Linux 2.1 ES Red Hat Enterprise Linux 2.1 WS Red Hat Enterprise Linux 3 AS Red Hat Enterprise Linux 3 ES Red Hat Enterprise Linux 3 WS Red Hat Enterprise Linux 4 AS Red Hat Enterprise Linux 4 ES Red Hat Enterprise Linux 4WS	32 bit x86 32 bit x86 32 bit x86 32 bit x86 32 bit x86 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 and Itanium 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86 32 bit x86 and 64 bit x86
SUSE Linux	SUSE Linux Enterprise Server 8 SUSE Linux Standard Server 8 SUSE Linux Enterprise Server 9	32 bit x86 32 bit x86 32 bit x86 and 64 bit x86

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

Supported Operating Systems for SAS Client	Versions	Architecture
Windows	Windows XP Windows 2003 Windows 2000	32 bit x86 32 bit x86 32 bit x86

Java J2SE v 1.4.2 must be installed on the system that runs on the SAS Client. To download this version of Java, go to http://java.sun.com/j2se/1.4.2/download.html.

Supported Core Operating Systems

The following table lists the supported operating systems for the Opsware core components (other than the Global File System Server). The Global File System server can be installed only on Red Hat Enterprise Linux 3 AS. Therefore, a single-server installation is supported only on Red Hat Enterprise Linux 3 AS.

Supported Operating System for Opsware Core	Versions
Sun Solaris	Solaris 8 (on SPARC) Solaris 9 (on SPARC)
Red Hat Linux	Red Hat Enterprise Linux 3AS (32 bit)

The following table lists the supported operating systems for the Opsware Satellite.

Supported Operating System for Opsware Satellite	Versions
Sun Solaris	Solaris 9 (on SPARC)
Red Hat Linux	Red Hat Enterprise Linux 3AS (32 bit)
SUSE Linux	SUSE Linux Enterprise Server 9 (32 bit)

The Data Center Intelligence Server runs on Windows 2000 and 2003.

Operating System Deprecation and End of Support

When a managed operating system is “end of life” by the operating system vendor, Opsware marks the operating system as deprecated as an indication that the operating system might be dropped from the list of supported managed operating systems in a future release of the SAS product.

Deprecated operating systems are supported in the current release of the product in the same way non deprecated operating systems are.

Opsware monitors operating systems usage by its customers on an ongoing basis and bases the operating system retirement decisions on operating system usage by current customers.

If you have any questions related to the Opsware operating system deprecation policy, please contact Opsware support or your account manager.

The following operating system versions are being deprecated in Opsware SAS 6:

- Red Hat Linux 7.3
- Red Hat Linux 8.0

(These operating systems have been deprecated since Opsware SAS 5.5.)

The following operating system versions are no longer supported in Opsware SAS 6:

- Red Hat Linux 6.2
- Red Hat Linux 7.1
- Red Hat Linux 7.2

(These operating systems have been deprecated since Opsware SAS 5.5.)

Supported Installations for Opsware SAS 6

The Opsware SAS 6 release supports the following installations:

- New installations of a standalone core
- New installations of a multimaster core
- New installations of a Satellite

Documentation for Opsware SAS 6

This release comes with the following documentation:

- *Opsware SAS 6 Release Notes*
- *Opsware SAS 6 Planning and Installation Guide*
- *Opsware SAS 6 Policy Setter's Guide*
- *Opsware SAS 6 Administration Guide*
- *Opsware SAS 6 User's Guide: Server Automation*
- *Opsware SAS 6 User's Guide: Application Automation*

- *Opsware SAS 6 Content Utilities 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 site.

Opsware SAS Web Services API 1.0 Retirement

Beginning with Opsware SAS 6, the Opsware SAS Web Services API 1.0 has been retired and is no longer available. Customers using Web Services API 1.0 have been contacted individually.

Known Problems, Restrictions, and Workarounds in Opsware SAS 6

This section describes the workarounds to known problems in Opsware SAS 6.

Application Configuration

Bug ID: 134791

Description: Error dialog displays when selecting Configured Application in some Server Browser Windows.

Platform: Any

Subsystem: Application Configuration/Server Explorer

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

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

Bug ID: 135209

Description: You cannot edit a recurring application configuration push job from Jobs and Sessions -> Recurring Schedules in the SAS Client.

Platform: Any

Subsystem: Application Configuration/Recurring Schedules

Symptom: From inside the SAS Client, from the Navigation Pane | Jobs and Sessions | Recurring Schedules, you are able to see recurring application configuration jobs, but you are not able to edit them.

Workaround: None.

Audit and Remediation

Bug ID: 136718

Description: In a small number of cases, some audit rule checks for a registry keys cannot be remediated if key is not present on target server.

Platform: Windows 2003

Symptom: When executing some audits using a custom check that checks a registry key, if that registry key is not present, then you will get an error describing "no key found" and you will not be able to remediate the value. Note that this only affects a small subset of registry checks.

Workaround: Manually create the specified registry key and the audit remediation will work correctly.

Bug IDs: 137901, 137904

Description: Text for "contains" and “does not contain” operators in the Application Configuration rule description in Audits during an Audit failure doesn’t fully explain feature correctly.

Platform: Any

Symptom: In the Application Configuration rule of the Audit and Remediation feature, the textual representations of rules that use the "contains" and "does not contain" operator are slightly misleading.

The following descriptions of these operators:

...there is an entry where <name> is containing value <value>

...there is an entry where <name> is not containing value <value>

incorrectly suggests that a specific element contains the value specified. What this operator actually does, however is to check that the entire file contains (or does not contain) an entry with the specified value.

Workaround: None.

Bug ID: 137898

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

Platform: Any

Subsystem: Audit and Remediation

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

Workaround:

1) Get the Windows utilities (showpriv.exe, ntrights.exe, auditpol.exe) from the Microsoft Windows 2000 Resource Kit.

2) Install the OCLI on a UNIX server managed by Opsware, or on an Opsware core server.

3) Copy the Windows utilities to /var/tmp on the UNIX server.

4) Make sure /opt/opsware/agent/bin is at the beginning of the PATH
e.g. export PATH=/opt/opsware/agent/bin:$PATH

5) Run the following three OCLI commands:

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

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

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

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

a) Using OCCC, go to Opsware Administration.

b) Go to 'Patch Settings'

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

Bug ID: 138010

Description: Deleting Snapshots and Application Configurations can result in undesired deletion of data.

Subsystem: Audit and Remediation (and Application Configuration)

Platform: Any

Symptom: Deleting an Audit and Remediation Snapshot will result in the deletion of data that the user does not want deleted. This also applies to the Application Configuration feature, specifically, if you have done an application configuration push, do not disassociate the application configuration from the server or server group.

Workaround: After you run a Snapshot job, do not delete the Snapshot. And, do not disassociate the application configuration from a server or server group after a push.

DCML Exchange Tool (DET)

Bug ID: 130600

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

Platform: Any

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.

Global Shell

Bug ID: 129237

Description: Error when you open a terminal window for a Windows or Unix server.

Subsystem: OCC Client – Remote Terminal, Global Shell

Platform: Independent

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

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

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

Bug ID: 129501

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

Subsystem: OCC 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: OCC Client - Global Shell

Platform: Windows

Symptom: In a Global Shell session, a non-admin user has permission to view the `/opsw/@/<server>/metabase` subdirectory of OGFS. However, the user cannot browse metabase, and the session displays the message `"Protocol error."`

In the agent.err file, the following lines appear:

```
<timestamp> [10997] ERR  Error from Agent for unique <int>:
. . .
File ".\base\ops\shell\ogfs_wshandler.py", line 402, in run
File ".\base\ops\shell\metabase.py", line 72, in
metabase_getattr
```

Workaround: Login as a member of the Administrators group (admin).

Bug ID: 132935

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

Subsystem: OCC Client - Global Shell

Platform: Independent

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

Workaround: Enter the following command:

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

Bug ID: 137220

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

Subsystem: OGFS Backend

Platform: Linux

Symptom: This problem occurs on the core server where the OGFS is installed, when you log into the core server and try to change the password of a Unix user with the passwd program. If you do not specify –r for passwd, the following error appears: "Unsupported nsswitch entry for passwd:. Use -r repository . Unexpected failure. Password file/table unchanged." The Opsware PAM module is installed on the core server where the OGFS component is installed. Because the Opsware PAM module alters /etc/nsswitch.conf, the passwd program needs the –r option to function correctly.

Workaround: Specify the –r option, for example:

% passwd -r files username

Bug ID: 136129

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

Subsystem: Global File System Backend

Platform: Windows

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

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

Bug ID: 137821

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

Subsystem: OCC Client – Global Shell

Platform: Solaris

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

Workaround: Change server attributes with the Opsware SAS Client.

Intelligent Software Module (ISM) Development Kit

Bug ID: 135249

Description: Cannot upload an ISM with passthru ZIP file on non-Windows platforms.

Platform: Linux

Subsystem: ISMTool upload

Summary: During the upload with ISMTool, the following error message appears:

> Error: passthru package hongtest6-ism-1.0.0-1.i386.rpm is not a valid package for the current platform Red Hat Enterprise Linux AS 4.

Workaround: Use RPMs for passthru packages.

Bug ID: 135455

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

Platform: 64-bit Windows

Subsystem: ISM

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

Workaround: None.

Operating System Provisioning

Bug ID: 130844

Description: Not setting up Windows 2003 R2 components results in a message dialog box.

Platform: Windows 2003 R2

Subsystem: OS Provisioning

Symptom: If you try to provision a server with Windows 2003, and did not add the proper Windows 2003 R2 information in the unattend.txt file, after the provisioning is finished and you log on to the server, you will be asked for the second installation disk ion order to complete the OS installation.

Workaround: Refer to the Windows 2003 R2 documentation for details on automating Windows 2003 R2 setup.

Bug ID: 136413

Description: Cannot copy an OS Sequence.

Platform: Any

Subsystem: OS Provisioning

Symptom: If you attempt to copy an OS Sequence, none of the information in the original OS Sequence will be copied to the new one and it will not be editable or usable.

Workaround: None.

Bug ID: 137956

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

Platform: Red Hat Linux Enterprise Linux 4 AS

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

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

Opsware Agent

Bug ID: 129395

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

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

Platform: Platform Independent

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

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

Bug ID: 129735

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

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

Platform: 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: 134405

Description: When installing an Opsware Agent on a Windows 2003 64-bit server, **t**he ODAD feature cannot load the enhanced Microsoft Crypto Service Provider (CSP) and writes an error to the Installer log file.

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

Platform: Windows 2003 64-bit

Symptom: On Windows 2003 x64, the Windows Agent installer is failing to checksum any version of the file ogshcap.dll already installed on the local system. The Windows Agent Installer writes the following error messages in the Installer log file:

```
[15/May/2006 18:25:16] [ERROR] Error calling
CryptAcquireContext: -2146893795
[15/May/2006 18:25:16] [ERROR] Error calling
CryptReleaseContext: 87
```

Workaround: Reboot the server after the ODAD finishes installing the Opsware Agent to guarantee that the latest version of the ogshcap.dll is installed and in use on the system.

Bug ID: 137558

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

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

Subsystem: Opsware Discovery and Agent Deployment (ODAD)

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

Workaround:

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

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

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

1. On the Windows Firewall window, select the Exceptions tab. Select the "File and Printer Sharing" service and click Edit. The Edit a Service window appears.

2. If not already selected, select the check box for port TCP 139. The default scope setting for this port is "Subnet."
3. When the Opsware Agent Deployment Helper server and target Windows server are on different subnets, click the "Change scope" button and change the scope of the port to "Any computer" or enter a user specified custom list.
4. Click OK to save your configuration changes.

Opsware Installer

Bug ID: 134512

Description: Startup of the Opsware SAS components fails when DHCP is not configured for the Opsware SAS core.

Subsystem: DHCP and the Opsware SAS Start Script

Platform: Independent

Symptom: If DHCP is not configured, starting and stopping this component results in a non-zero exit status from the init script, which the Opsware SAS Start Script interprets as an error, and other Opsware SAS components will not start.

Workaround: Run the Opsware SAS DHCP Configuration Tool to configure DHCP for the Opsware SAS OS Provisioning feature. See the Opsware SAS 6.0 Installation Guide for information. Alternatively, you can enter the following command to workaround this issue:

```
chmod 000 /etc/opt/opsware/startup/dhcpd
```

Bug ID: 137740

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

Subsystem: Opsware Global File System Server (OGFS)

Platform: Independent

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

Workaround:

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

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

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

(2) Start the OGFS component by performing the following steps:

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

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

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

Opsware SAS Client

Bug ID: 135932

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

Subsystem: SAS Client - Search

Platform: Platform Independent

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

Source / Target Server

Source/Target Server Asset Tag

Source/Target Server Serial Number

Source/ Target Snapshot Name

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

Workaround: None

Bug ID: 137536

Description: Unable to view the job details for a Visual Packager job in the SAS Client.

Subsystem: SAS Client - Visual Packager

Platform: Platform Independent

Symptom: When you use the Job Logs in the SAS Client to review the job information for a Visual Packager Job, you are unable to view the job details for a Visual Packager Job.

Workaround: None

Bug ID: 137634

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

Subsystem: SAS Client - Search

Platform: Platform Independent

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

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

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

Patch Management

Bug ID: 132400

Description: You have a server running Service Pack 3. When you try to remediate a patch policy that contains patch1 (for SP3), patch2 (for SP4), and Service Pack 4, only patch1 and Service Pack 4 will be installed. Since patch2 is intended for SP4, it will not get installed because when you start the remediate process, the server is still at SP3. After the first remediate is complete and you run the remediate process again, patch2 will then get installed.

Platform: Windows

Subsystem: Opsware SAS Client – Patch Management for Windows

Symptom: You have a patch policy attached to a server running Service Pack 3. The patch policy contains patch1 (for SP3), patch2 (for SP4), and Service Pack 4. When you run the remediate process, only patch1 and Service Pack 4 are installed. After the remediate process is complete and you run the remediate process again, patch2 will then get installed.

Workaround: If a Service Pack or a patch that is dependent on a certain Service Pack needs to be installed, install it manually. Do not use the remediate process to install a patch or a Service Pack that is dependent on a certain Service Pack.

Bug ID: 132415

Description: Email notifications were not sent when the install, uninstall, or remediate process failed due to pre-install or pre-uninstall scripts that failed to run.

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

Symptom: You tried to install a patch where the pre-install or pre-uninstall script failed. No email notifications were sent.

Workaround: None.

Bug ID: 132467

Description: You cannot use the SAS Client to uninstall a patch that was installed with the OCC application node.

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

Symptom: You created an application node and added a patch to it. In the OCC, you installed the application node on a managed server. In the OCC, you removed the application node from the server. In the SAS Client, you tried to uninstall it with the Uninstall Patch task window and received an error explaining that “This patch cannot be uninstalled because it is referenced by another part of the model.”

Workaround: Use the SAS Client for all Windows patching.

Bug ID: 132599

Description: In the Properties view that lists patches for a certain Windows operating system, a patch is displayed as grayed out when Patch Management cannot determine whether the version of the patch that is installed is the same as the version of the patch that is in the Library. This occurs when the GUID identifier is not provided or is the same for both versions of the patch.

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

Symptom: A patch install appears successful; however, after verification, Opsware determined that the patch was not actually installed. When you view patches listed for a certain operating system in the Properties view, you see two patches displayed: one is grayed out and shown as installed-not-by-opsware and one is not installed.

Workaround: None.

Bug ID: 132863

Description: Even though one version of a patch is already installed on a server, it is possible that the vendor will recommend that another version of the same patch should be installed. In this case, Patch Management indicates only that the patch is recommended. Patch Management does not indicate that the patch is both (already) installed and recommended.

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

Symptom: A version of a patch is already installed on a server and there is no black check mark in the Installed column in the All Managed Servers preview pane. After you install a different version of the patch (because the patch was recommended by the vendor), Patch Management reports that the two version of the patch are now installed.

Workaround: None.

Bug ID: 132866

Description: When you add an Update Rollup to a patch policy, not all versions of it are added. Only the Update Rollup you selected will be added.

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

Symptom: You tried to add all versions on an Update Rollup to a patch policy. Only the version of the Update Rollup you selected was added.

Workaround: Manually add all versions of the Update Rollup to a patch policy.

Bug ID: 132907

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

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

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

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

Bug ID: 137157

Description: Patching did not continue after reboot.

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

Symptom: The Agent is unable to report a complete set of installed and recommended patches because the Automatic Updates service is disabled. Patching relies on the MBSA 2.0 scanning engine (mbsacli) to detect installed and recommended patches. If the Automatic Update service is disabled, mbsacli will not work properly and the patching process will not continue after reboot.

Workaround: Verify that the Automatic Updates service is enabled. The MBSA analysis tool is the executable that is used by WindowsUpdate to identify the patches required.

Bug ID: 137322

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

Platform: Windows

Subsystem: SAS Client – Patch Management for Windows

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

Workaround: None.

Reports

Bug ID: 133350

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

Platform: Independent

Subsystem: SAS Client – Reports

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

Workaround: Click the “Show all <nn> servers” link to view the correct multi-byte characters.

Bug ID: 133351

Description: No report results display when you click the multi-byte character link.

Platform: Independent

Subsystem: SAS Client – Reports

Symptom: When you click the multi-byte character link, no report results are displayed. The report should return the same number of objects as indicated in the link.

Workaround: Click the “Show all <nn> servers” link to view the correct multi-byte characters.

Bug ID: 133652

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

Platform: Independent

Subsystem: SAS Client – Reports

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

Workaround: See the information displayed in the Customer column.

Software Management

Bug ID: 137610

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

Subsystem: SAS Client - Software Management

Platform: Independent

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

Workaround: None.

Bug ID: 134892

Description: Sometimes you are unable to install a software policy template on a managed server using the Software Policy Template window.

Subsystem: SAS Client - Software Management

Platform: Independent

Symptom: When you install a software policy template on a managed server using the Install Software Policy Template window, the Next button is disabled after you have selected the software policy templates to be installed on a server. As a result, you are unable to continue the task of installing the software policy template. This behavior is observed intermittently.

Workaround: Log out of the SAS Client and then log back in to the SAS Client. You can now install a software policy template to a managed server by using the Install Software Policy Template window.

Visual Application Manager

Bug ID: 136430

Description: Sometimes when a Visual Application Manager window opens for a new scan, one of the nodes in the Network View is oversized (in height or width).

Platform: Independent

Subsystem: SAS Client – Visual Application Manager

Symptom: In the Network View, one server node is at least 100 times taller than the normal (default) size. All other nodes are sized properly. In the Server View, the same server node is the default size.

Workaround: From the View menu, select the Reset Graph Layout option to restore all nodes in the view to their default size.

Bug ID**:** 137955

Description: Only the currently viewed topology and the application are saved.

Platform: Independent

Subsystem: SAS Client – Visual Application Manager

Symptom:

1. Create a .vam file and save multiple topologies in it.
2. Reopen this file.
3. Use the Save As action and overwrite the original file.

The expected results would be that the application is saved as if the Save action had been performed. The actual results are that only the currently viewed topology and the application are saved. It treats the current scan and application as if it were completely new. Note that this will currently only work for local files. Trying this for a file on the hub will cause an exception with the result that the old data is left as a backup file (~<name>.vam.bak).

Workaround: Click the Save button, regardless of whether the file is on the hub or local.

Contacting Technical Support

To contact Opsware Technical Support:

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

E-mail: support@opsware.com

For information about Opsware Technical Support:

URL: https://download.opsware.com

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