HP Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 7.81

SA 7.81 Release Notes

Document Release Date: November 2009
Software Release Date: November 2009

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Intel® Itanium® is a trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://support.openview.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Document Changes

Chapter	Date	Changes
	November 2009	Document Created

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 New in SA 7.81

Critical Defect Fixes

The following defects were fixed in 7.81:

Table 1 Critical Defect Fixes in SA 7.81

QCCRID	Description
70583/159229	Random user actions sometimes cause `HTTP Status 500` in the SA Web Client.
72251	Remediating a software policy that contains a package that was previously manually installed results in an incorrect error message.
73612	The Audit option `Archive full file contents` is misleading.
76594	Should be able to trigger reboots immediately after running a script in a software policy.
79697	The Windows Patch Management database incorrectly identifies required patches.
82756	Agent Deployment fails on Solaris servers when using csh shell.
83067	Agent for VMWare ESX 4 does not read the RAM size as expected.
83143	Improved error message required when the file tadnsw.exe is missing.
83222	Conflict resolution operations should have smaller impact on performance.
83968	When Windows servers with no recommended patches are scanned for addition to an SA Core, they are not moved out of the `Scan Needed` state.
84111	In the Device Group browser, when you select Device Membership and choose the Import option to import servers through a CSV file, you are unable to change focus to another window.
84313	When a Windows 2008 server with an IIS role enabled is visualized, it is shown as an unconnected process.
88615	Remediate should handle RPM dependencies more intelligently when remediating detached software policies.
89237	Provisioning a VMWare ESX 3.5 VM with Windows Server 2008 fails due to permission issues.
89739	Internationalization (I18N) on VMWare ESX: Create or Modify VM options do not work with non-ASCII characters in the name/description.
90094	Need to add support for new version of HP NC-Series Broadcom 1Gb Driver for Windows Server 2003.

Table 1 Critical Defect Fixes in SA 7.81 (cont'd)

QCCRID	Description
90201	The Powershell cmdlet fails with the error `Set-SasServer : No such operation 'update'`.
90509	The Windows Patching option **Right Click ➤ Set Availability** does not save the availability status.
90586	Improve error message when an Application Installation Media (AIM) install script exits with non-zero exit code.
90961	Compliance Check Editor: Update cache events are not generated when compliance checks properties are modified.
91806	A Solaris patch policy attached through a device group does not show inherited icon and tooltip.
92173	The DCML Exchange tool (DET/CBT) does not update platform associations for units on second import after an export using the `-incr` argument.
92264	The Agent Deployment Tool (ADT) fails on a Virtuozzo host with the error: Agent port in use.
92308	Software Policies that contains patches that supersede other patches in the same policy can cause remediation failures.
92426	A Solaris local zone's Installed Patches list does not show a patch that was installed through a Patch Policy remediated at the global zone level.
92622	System uses the wrong IP address to contact the core on a system with virtual IPs on same subnet.
92819	The Web Services Data Access Engine (twist) consumes 100% CPU.
92829	Snapshots for the software discovery inventory fail on HP-UX with the error: `unknown encoding: iso88591`.
92982	An Advanced Search using the Agent Discovery Date Between rule creates a dynamic group with incorrect date values.
93055	In the Server Browser, the Hyper-V periodical scan history is incorrectly referred to as a VMWare ESX scan.
93123	When running Create VM with an old Create VM job window open, the Create VM job fails with a duplicate name error.
93128	If you re-open an OS Sequence with pre-/post-remediate script run as root the Name/Password/Domain fields become editable.
93159	A query on the Job Table does not return the correct results when a job ID is specified in the filter.
93169	Create Zone Agent installations fail with the error: `/opt/opsware/agent/pylibs/coglib/wordclient.pyc: [Errno 2] No such file or directory`.

Table 1 Critical Defect Fixes in SA 7.81 (cont'd)

QCCRID	Description
93173	When viewing installed packages in a snapshot of a Red Hat Enterprise Linux 5.0 server using the Server Browser, 32-bit and 64-bit packages with the same package name are shown as a single entry.
93220	After discovering a VMWare ESX VM, a virtual server refresh generates the Java console exception: `AWT-EventQueue-0" java.lang.ArrayIndexOutOfBoundsException: 14 > 13`.
93225	Modification of a platform in a Solaris patch policy is not validated against the platforms of the servers attached to the policy.
93309	After an ad hoc User Group installation, if the user group name does not follow Solaris naming conventions, the job status shows as `Not Installed` even though the user group has been installed.
93393	Patch scan fails if a server has an exception for a patch in policy attached to the server and the server's device group.
93496	The timeout for installing a Windows hotfix should be reduced from the current 60 minutes.
93589	Cannot change the size of disk being added to a VM in a powered-on state.
93600	In a multimaster mesh in a very large Facility with a large amount server data, the MBC/DHCPD Tool takes several minutes to process input.
93633	Snapshots size is too large.
93703	Attempting to create a virtual machine (VM) and provision an OS on a virtual machine without installing a network interface (NIC), SA creates multiple VMs until it runs out of resources.
93756	In a Solaris 10 hypervisor History view, a recurring scan event is not logged.
93847	Windows Server 2008 OS provisioning fails due to inability to resolve hostnames.
93935	Document how to configure `ssh`, `rlogin`, and `telnet` clients for remote login to unmanaged servers ADT remote login.
93940	Windows agent authentication system is missing from some Windows servers after agent is successfully installed.
93982	The Gateway (`opswgw`) chroot environment on Linux x86_64 is missing the `/lib64` directory.
94076	Creating or modifying multiple VMs at nearly the same time fails on VMWare ESX and ESXi.
94119	Running a snapshot with the Perform Inventory option on VMWare ESX servers, an error occurs indicating that the database installation appears to be corrupted.
94127	Software policy remediation attempts to install Windows user/group object on a Solaris server and fails.

Table 1 Critical Defect Fixes in SA 7.81 (cont'd)

QCCRID	Description
94132	A Windows server's Recommended Patches list may not display certain patches as recommended even though the patches are recommended by the patch scanning engine.
94207	VMWare ESX feature Open Console does not work.
94277	URL for the deployed web services is invalid.
94338	Program APXs do not have a configurable concurrency setting.
94379	Application Configuration provisioning hangs.
94420	Running a program APX on multiple servers with multiple Slices Component bundles yields a undesirable Slice distribution.
94467	Implement the capability to export audit results as an XML or JSON file.
95403	SMOs should allow values to be added/changed for certain audit parameters, for example, `Account Lockout Threshold`.
95735	Remote commands can take too log to initiate in a remote datacenter.
95918	The physical memory in a Windows VM created by Microsoft Hyper-V is not correctly determined.
96839	Software compliance is always shown as `Non-compliant` if there is an application configuration in the Software Policy.
97634	Reports for Application Configuration can have incorrect or mismatched session ID and Compliance Summary data.
97790	Reports for Software Management can have incorrect or mismatched session ID and Compliance Summary data.
97792	Reports for Patch Management can have incorrect or mismatched session ID in the compliance summary table.
98995	Need `OGSH/ROSH` support in Solaris 8 & 9 branded zones running in Solaris 10 SPARC containers.
99173	Audit results in the Details window are labeled with the wrong color (blue instead of red) and Java console errors occur.
99364	Manage Boot Client (MBC) DHCPd cleanup fails to load when the facility short name is different from the facility display name.
99537	If an audit has one non-compliant setting within a rule that has multiple checks, all checks are marked as non-compliant.
99603	OS Provisioning Media Server import fails to import Windows Server 2008 SP2 media.
99604	Should support Windows 2008 Server R2 as a managed platform.
100053	Solaris agent does not report MAC address.
100078	ZIP installation paths - allow special characters in environment variables for Windows x64 versions.

Table 1 Critical Defect Fixes in SA 7.81 (cont'd)

QCCRID	Description
100395	Software Compliance does not work correctly when there are two RPMs with the same name but different versions on the same server.
100396	Software Compliance does not work correctly on x86_64 platforms.
100417	When there are old and new versions of the same rpm on a server, rpms with versions in between are not compliant.
100563	Multiple vnodes pointing to the same inode.
100854	`Continue on Errors` option does not work when remediating a Software Policy with an application configuration.

Supported Operating Systems

For a complete list of supported platforms for SA 7.81 Cores, Agents, and Satellites, see the *SA Supported Platforms* provided with the SA documentation.For information about deprecated operating systems, see your 7.80 *SA Planning and Installation Guide* or *SA Upgrade Guide.*

Microsoft Hyper-V Virtual Machine Enhancements

This version of HP Server Automation significantly improves and expands your ability to manage Hyper-V hypervisors and virtual machines (partitions). With this version of SA you can create and provision Hyper-V virtual machines with these operating systems:

- Windows Server 2008 x64 and x86
- Windows Server 2003 x86
- Windows Server 2000
- Windows XP Professional x86 SP 2 or SP 3
- SUSE Linux Enterprise Server 10 with Service Pack 2 (x86 or x64 Edition)
- SUSE Linux Enterprise Server 10 with Service Pack 1 (x86 or x64 Edition)

You can also modify and delete Hyper-V VMs. You can add, delete and modify the following on Hyper-V VMs:

- Legacy Network Adapters
- Network Adapters
- SCSI Controllers
- Virtual Hard Disks
- DVDs

You can also modify the following on Hyper-V VMs:

- Memory size
- The number of virtual processors
- BIOS order
- VLAN and MAC address configuration of network adapters
- Media specification for DVDs
- Controller and location for virtual hard disks

For complete information, see "Microsoft Hyper-V Partition Management" in the *SA User's Guide: Server Automation*.

Solaris Patching Enhancements

This version of HP Server Automation significantly improves the process of keeping your Sun Solaris servers running with current patches. With this version of SA you can:

- Determine which patches your managed servers need.
- Download Solaris patches and patch clusters and store them in the SA library.
- Create Solaris patch policies from downloaded Solaris patches and patch clusters.
- Resolve all the dependencies for a set of patches including required patches, obsolete patches, superseding patches, incompatible and withdrawn patches.
- Install patches and patch clusters by remediating patch policies on managed Solaris servers. Remediation automatically handles various patch reboot settings including single-user mode, reconfiguration reboot and reboot immediate.

For complete information, see "Patch Management for Solaris" in the *SA User's Guide: Application Automation*.

New Platform Support for Managed Servers

Table 2 lists all new operating system support for managed servers in SA 7.81.

For more detailed descriptions of supported system configurations, see the SA 7.81 Supported Platforms Matrix.

Table 2 Platform Support for Managed Servers in SA 7.81

Operating System	Version
Windows	Windows Server 2008 R2 (Standard, Enterprise, Datacenter) Windows Server 2008 (Standard, Enterprise, Datacenter, Web)
CentOS	CentOS 5
Oracle	Oracle Enterprise Linux 5

Table 2 Platform Support for Managed Servers in SA 7.81 (cont'd)

Operating System	Version
Linux	SuSE Linux Enterprise Server 11
Sun	Solaris 10 U7
VMware	ESX Server 4.0 ESXi Server 4.0 Embedded ESXi Server 4.0 Installable

Revised Sizing Guidelines

SA 7.80 and later have increased memory demands on the Slice Component bundle host(s). Table 3 and Table 4 provide the revised sizing guidelines:

Table 3 Small-to-Medium SA Deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server		
	Server 1*	**Server 2***	**Server 3****
500	MR, Infra, Slice 0, OS Prov	N/A	N/A
1000	MR	Infra, Slice 0, OS Prov	N/A
	N/A	N/A	MR, Infra, Slice 0, OS Prov

* Server Configuration: 4 CPU cores, 8 GB RAM, 1 GB/s network

** Server Configuration: 8 CPU cores, 16 GB RAM, 1 GB/s network

Table 4 Medium-to-Large SA Deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server				
	Server 1*	**Server 2***	**Server 3***	**Server 4***	**Server 5***
2000	MR	Infra, Slice 0, OS Prov	N/A	N/A	N/A
4000	MR	Infra, Slice 0, OS Prov	Slice 1	N/A	N/A

Table 4 Medium-to-Large SA Deployment (SA 7.80 and later) (cont'd)

Managed Servers	SA Component Distribution by Server				
6000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	N/A
8000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	Slice 3
* Server Configuration: 8 CPU Cores, 8 GB RAM, 1 GB/s network					

Windows Agent Deployment Helper Obsolete

In SA 7.81, the *Windows Agent Deployment Helper (WADH)* is no longer required to manage Windows servers with SA and has been removed from the SA distribution.The process of bringing Windows servers under SA management is now the same as for any other platform.

After you install this patch on all your core and satellite servers and are certain that you will not need to roll back the 7.81 patch, you can redeploy the Windows server that hosted the WADH.

The removal of WADH obsoletes the following sections in the SA 7.80 documentation set:

- The WADH installation instructions described under "Enabling ODAD for Windows Servers" on pages 118-119 of the 7.80 *SA Planning and Installation Guide* are no longer required.
- The bullet on page 35 of the *SA Policy Setter's Guide* that reads:

  The folder contains the tools required to install the Windows Agent Deployment Helper and upload ISMs to SA.

  See the *SA Planning and Installation Guide* for more information about Windows Agent Deployment Helper. See the *SA Content Utilities Guide* for more information about ISMs.

  is no longer valid. This change also affects online help.
- Step 1 under "Discovery and Agent Deployment" on page 28 of the 7.80 *SA Administration Guide* is no longer required.
- Step 6a under the heading "For Windows:" on page 28 of the 7.80 *SA Administration Guide* is no longer required.
- On page 208 of the 7.80 *SA Administration Guide* the permissions requirements should be:
  - Read access to facilities where you will scan for servers and manage servers.
  - **Features ➤ Managed Servers and Groups** must be enabled.
  - **Client Features ➤ Unmanaged Servers ➤ Allow Manage Server** set to Yes.
  - **Client Features ➤ Unmanaged Servers ➤ Allow Scan Network** set to Yes.
  - Read access must be set to customer `Opsware`.

  The last five Read permissions listed on page 208 are no longer required.

- The WADH permissions listed in Table 31: “Default Top-Level Folder Permissions of the Predefined User Groups” on page 262 of the 7.80 *SA Administration Guide* are no longer required.
- The section “Prerequisite Setup for Discovery and Agent Deployment” on page 88 of the 7.80 *SA User’s Guide: Server Automation* and in the SA online help is no longer required.
- In the 7.80 *SA User’s Guide: Server Automation* section titled “Creating Reports on Agent Installation,” the Example Report on page 95 is no longer valid.
- The requirement to install a WADH displayed in the section “Deploying Server Agents on Unmanaged Servers” in the SA online help is no longer valid.

Agent Deployment Tool (ADT) Behavior in a Mixed-SA Version Environment

When you run the Agent Deployment Tool (ADT) from a 7.81 SA Client session (the SA version of the core the SA Client session is logged in to), Windows agent deployment from that session is supported only to realms also running SA 7.81; deployment to realms running earlier SA versions is not supported.

If SA Client session is logged into a pre-7.81 core (for example, 7.80, 7.50.03, etc.) as long as that SA core has a properly configured Windows Agent Deployment Helper server, you can deploy Windows agents from that session to realms running SA 7.81 as well as earlier versions.

Veritas File System Support - Red Hat Enterprise Linux SA Cores

As of SA 7.81, the Veritas File System (VxFS) is supported for SA Cores on Red Hat Enterprise Linux. Veritas File System (VxFS) *is not supported* on Solaris systems. For more information, see the *SA Supported Platforms* in the documentation directory of your SA installation.

Storage Visibility and Automation Feature

For Server Automation 7.81, the following changes were made to the Storage Visibility and Automation feature:

- Added new platforms that support the Storage Host Agent Extension component.
- Added new storage reports and moved these reports and the corresponding user documentation to the BSA Essentials Network (BSAEN) for delivery.
- Updated the storage compliance functionality and moved the corresponding user documentation for storage audits to the BSA Essentials Network (BSAEN) for delivery.
- Fixed and described product defects.
- Identified and described known product defects.

See the *Storage Visibility and Automation 7.81 Release Notes* for detailed information about these changes.

Documentation for SA 7.81

The following documentation are provided with this patch release:

- *SA Release Notes* for 7.81
- *SA User's Guide: Application Automation*
- *SA User's Guide: Server Automation*
- *SA Policy Setter's Guide*
- *SA Platform Developer's Guide*
- *SA Supported Platforms*
- *SA Open Source and Third-Party Software Acknowledgements*

The following SA 7.80 documents are still valid for this patch release:

- *SA Oracle Setup for the Model Repository*
- *SA Content Utilities Guide*
- *SA Content Migration Guide*

2 Installing SA 7.81

This section describes the procedure to install SA 7.81.

SA 7.81 Core and Satellite Software Installation Procedure

General Information

- SA 7.81 can be rolled back, but only to the previous full release. Therefore, SA 7.81 can be rolled back to SA 7.80.
- The `patch_opsware.sh` script is used both for installing and for uninstalling SA 7.81.
- There's no need to supply a response file with `patch_opsware.sh`.
- This patch includes updated Server Agents that will be uploaded to the Software Repository. However, no agents will be upgraded on core machines (that is, in the Model Repository) or on Managed Servers without manual intervention
- SA 7.81 can only be installed on systems running SA versions with a Build ID of `opsware_37.0.3006.*`.

  If any installed SA components (other than a previously installed patch) have a different build ID, you won't be allowed to install this patch.

  To determine the build ID for a core machine, open the file

  `/var/opt/opsware/install_opsware/inv/install.inv`

  and find the section beginning with `%basics_`. Under this line, find the `build_id`. For example:

  ```
  %basics_linux
  build_id: opsware_37.0.3006.*
  ```

  When you install an SA patch, the patch installation updates the `install.inv` file to record the patch installation and the patch build ID. For example:

  ```
  %opsware_patch
  build_id: opsware_37.0.3826.0
  ```
- Before a patch operation (such as install/upgrade/uninstall), all core/satellite services must be up and running. If any services are stopped or dysfunctional (as reported by the `/etc/init.d/opsware-sas status` command), the patch operation will terminate.
- Upon completion of a patch operation, all services on the core/satellite machine should be up and running.
- If you are patching a multi-host core/satellite, you must patch each core and satellite host separately, one at a time, in any order.

- If you are patching a Multi-master mesh, HP recommends that you patch the primary core first, followed by secondary cores and satellites, thus ensuring that the primary core is at a higher version (such as SA 7.81 or higher) than the secondary cores.

  If you must roll back the SA 7.81 patch in a Multi-master Mesh, HP recommends that you roll back the secondary cores and satellites first, then the primary core.

- In order to patch and/or roll back Wayscripts, the `spog.pkcs8` certificate must exist under `/var/opt/opsware/crypto` (typically the certificate is installed with the Shell, SAS Web Client, or Build Manager). If the certificate does not exist, the patch operation will fail with the following error:

  ```
  Could not find spog.pkcs8 /var/opt/opsware/crypto
  ```

  Please copy the certificate from another core machine (for example, `occ`) to `/var/opt/opsware/crypto/oi` and retry this operation.

  If this error is encountered, simply copy the certificate from another core machine to your core server and retry the operation.

- In order to patch and/or roll back Software Repository (`word`) updates, the `spin.srv` certificate must exist under `/var/opt/opsware/crypto` (typically the certificate is installed with the Web Services Data Access Engine (`spin`)). If the certificate does not exist, the patch operation will fail with the following error:

  ```
  Could not find spin.srv under /var/opt/opsware/crypto.
  ```

  Please copy the certificate from another core machine (such as `occ`)to

  `/var/opt/opsware/crypto/oi`

  and retry this operation.

Pre-Patching Procedure

You must install an SA update on 7.80 cores before installing the SA 7.81 patch. This update enables the SA Core to handle new supported managed platforms introduced in CORD patch releases by ensuring mesh compatibility between a First Core patched with SA 7.81 and unpatched Secondary Cores.

The update should be applied to each Slice Component bundle host in all secondary cores and only needs to be applied once during the lifetime of the SA 7.80 server. If for some reason you have not applied the update, the CORD installation will automatically install the update before installing the CORD release.

This update cannot be rolled-back.

To install the pre-patch update, run the following command:

```
<distro>/opsware_installer/tools/prepatch.sh
```

If the patch has not been previously been applied, the following is displayed:

```
Patching /opt/opsware/occclient/ngui.jar
```

If the patch has been previously applied, the following will be displayed:

```
/opt/opsware/occclient/ngui.jar checksum = <current MD5 checksum>
Patch not applicable.
```

Installation Procedure

Perform the following tasks to install SA 7.81:

1. Mount the SA 7.81 distribution. Invoke `patch_opsware.sh` on every host in the core/satellite facility:

   ```
   <distro>/opsware_installer/patch_opsware.sh --verbose
   ```

   Usage: `patch_opsware.sh [--verbose]`

   `patch_opsware.sh` automatically detects whether or not there is a patch already installed and presents a corresponding menu:

   a. *Non-upgraded System*: If your system has not been upgraded, you see the following menu:

   ```
   Welcome to the Opsware Installer.
   It appears that you do not have any patches installed on this system.
   Press 'i' to proceed with patch installation.
   Press 's' to show patch contents.
   Press 'q' to quit.
   Selection:
   Enter "i" at the prompt to begin the installation.
   ```

   b. *Previously Upgraded System*: If an SA patch has already been installed successfully, when patch_opsware.sh is invoked from a newer patch release, you see the following menu:

   ```
   Welcome to the Opsware Installer.
   It appears that you have installed or attempted to install a previous
   version of the patch on this system.
   Press 'u' to upgrade the patch to the current version.
   Press 'r' to remove this patch.
   Press 's' to show patch contents.
   Press 'q' to quit.
   Selection:
   Enter "u" at the prompt to begin the upgrade.
   ```

2. After you make your selection, the installer completes the new (or interrupted) installation.

   The installer displays the following upon completion:

   ```
   [<timestamp>] Done with component Opsware Patch.
   [<timestamp>]
   ############################################################
   [<timestamp>] Opsware Installer ran successfully.
   [<timestamp>]
   ############################################################
   ```

Software Repository Content Upgrade

This section details upgrades to the software repository content on the upload distribution (such as agent packages to be reconciled to managed servers).

General Information

- Upgrading software repository content data is similar to using `patch_opsware.sh` from the upload distribution, but will only update those packages that have changed since the last major version.
- If you are upgrading a core hosted on multiple servers, the Software Repository content patch must be applied to the server hosting the Software Repository Store (`word store`).
- If you are upgrading a Multimaster Mesh, the Software Repository content upgrade should only be applied to the First Core (the upgraded content will automatically be propagated to other cores in the mesh).

Unlike core patches, Software Repository content upgrades cannot be rolled back.

Upgrading the First Core Content

1. On the First Core Software Repository store (`word store`) host, invoke the upgrade script:

   ```
   <distro>/opsware_installer/patch_contents.sh --verbose -r <response file>
   ```

   where `<response file>` is the response file last used to install/upgrade the SA Core.

   The following menu is displayed:

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.
   1 ( ) Software Repository - Content (install once per mesh)
   Enter a component number to toggle ('a' for all, 'n' for none).
   When ready, press 'c' to continue, or 'q' to quit.
   ```

2. Enter either `1` or `a` a and press `c` to begin the installation.

   If the Software Repository content image is not installed on the server, the following message will be displayed:

   ```
   [<timestamp>] There are no components to upgrade.
   [<timestamp>] Exiting Opsware Installer.
   ```

Rolling Back the Upgrade

To rollback SA 7.81 to SA 7.80, invoke the script:

```
<distro>/opsware_installer/patch_opsware.sh --verbose
```

If this is a patched system, the following will be displayed:

```
Welcome to the Opsware Installer.
It appears that you have previously completed installation of this patch on
this system.
Press 'r' to remove this patch.
Press 's' to show patch contents.
Press 'q' to quit
Selection:
Enter "r" at the prompt to remove the patch.
```

Notes:

- Rolling back SA 07.81 does not remove the Windows Server 2008 data that was created when the core was upgraded. For example, any Windows Server 2008 patches or policies created will remain. If you try to install these patches or attach the policies, an error will occur.
- Rolling back SA 7.81 does not delete any patches and policies that you have imported or created after the upgrade and these may fail with an error if you attempt to run them.

3 Fixed in SA 7.81

Agents

QCCRID 82756

Description: Agent Deployment fails on Solaris servers when using csh shell.

Platform: Solaris

Subsystem: Agent Deployment/Upgrade Backends

Symptom: Agent cannot be deployed to Solaris servers using csh shell. If the shell is set to bash or sh, the agent will be deployed without a problem.

Resolution: Fixed

QCCRID 92264

Description: The Agent Deployment Tool (ADT) fails on a Virtuozzo host with the error: `Agent port in use`.

Platform: Virtuozzo

Subsystem: Agent Deployment/Upgrade Backends

Symptom: ADT fails with the error: Agent port in use on Virtuozzo host which already has one of its guest container running an SA agent. ADT fails with the following error:

```
<timestamp>: Begin AgentPort test...
<timestamp>: {0} test failed
sh-3.00# \netstat -na | \grep ":1002 " | \grep LISTEN
tcp 0 0 0.0.0.0:1002 0.0.0.0:* LISTEN
```

Resolution: Fixed

QCCRID 93169

Description: Create Zone Agent installations fail with the error: `/opt/opsware/agent/pylibs/coglib/wordclient.pyc': [Errno 2] No such file or directory`.

Platform: Solaris 10

Subsystem: Agent

Symptom: For a Solaris 10 hypervisor whose agent is installed in a non-default directory, Create Zone job's install agent step fails with the error above.

Resolution: Fixed

QCCRID 93940

Description: Windows agent authentication system is missing from some Windows servers after agent is successfully installed.

Platform: Windows

Subsystem: Agent

Symptom: Windows agent authentication system is missing from some Windows servers after agent is successfully installed.

Resolution: Fixed

QCCRID 98995

Description: Need OGSH/ROSH support in Solaris 8 and 9 branded zones running in Solaris 10 SPARC containers.

Platform: Solaris 8 & Solaris 9

Subsystem: Agent

Symptom: Need OGSH/ROSH support in Solaris 8 and 9 branded zones running in Solaris 10 SPARC containers.

Resolution: Fixed

QCCRID 100053

Description: Solaris agent does not report MAC address.

Platform: Solaris

Subsystem: Agent

Symptom: Solaris agent does not report MAC address.

Resolution: Fixed

Application Automation Extensions (APXs)

QCCRID 93600

Description: In a multimaster mesh in a very large Facility with a large amount server data, the MBC/DHCPD Tool takes several minutes to process input.

Platform: VMWare ESX/Linux/Solaris

Subsystem: MBC/DHCPD

Symptom: In a multimaster mesh in a very large Facility with a large amount server data, the MBC/DHCPD Tool takes several minutes to process input.

Resolution: Fixed

QCCRID 99364

Description: Manage Boot Client (MBC) DHCPd cleanup fails to load when the facility short name is different from the facility display name.

Platform: Independent

Subsystem: APX - WebApp

Symptom: When the DHCP cleanup form tries to load, if the facility short name and display name differ, an exception is thrown.

Resolution: Fixed

Application Configuration

QCCRID 93633

Description: Snapshots size is too large.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: Snapshot size is too large and causes timeout errors.

Resolution: Fixed

Audit and Compliance

QCCRID 73612

Description: Audit with `Archive full file contents` selected always checks/remediates filesize and contents.

Platform: Independent

Subsystem: Audit and Compliance - Backend

Symptom: The label `Archive the full file contents` was misleading. The label should be changed to `Archive the file for remediation`. By design, you can only remediate a file audit where the source file was archived and the remediate always replaces the entire file.

Resolution: Fixed

QCCRID 97634

Description: Reports for Application Configuration can have incorrect or mismatched session ID and Compliance Summary data.

Platform: Independent

Subsystem: Application Configuration Backend

Symptom: Reports for Application Configuration can have incorrect or mismatched session ID and Compliance Summary data.

Resolution: Fixed

QCCRID 90961

Description: Compliance Check Editor: Update cache events are not generated when compliance checks properties are modified.

Platform: Independent

Subsystem: Audit & Compliance UI

Symptom: No update events are generated when compliance check properties are modified.

Resolution: Fixed

QCCRID 94467

Description: Implement the capability to export audit results as an XML or JSON file.

Platform: Independent

Subsystem: Audit & Compliance Backend

Symptom: You can now open an audit result and export the data as a JSON or XML file.

Resolution: Fixed

QCCRID 98718

Description: Audit that prints ASCII characters > 128 to `stdout` causes exception.

Platform: Windows

Subsystem: Audit and Compliance

Symptom: An audit will fail with an exception caused by an ASCII codec error.

Resolution: Fixed

QCCRID 99537

Description: If an audit has one non-compliant setting within a rule that has multiple checks, all checks are marked as non-compliant.

Platform: Independent

Subsystem: Audit & Compliance Backend

Symptom: When an audit is conducted and the results are checked, it appears that one non-compliant setting within a rule that has multiple checks will cause all the checks to be marked as non-compliant.

Resolution: Fixed

Command Engine (OCC)

QCCRID 83027

Description: Removing facility permissions does not reliably revoke users' ability to run a scan.

Platform: Independent

Subsystem: Command Engine - OCC CLient Framework

Symptom: Under certain circumstances, although a user's permissions for a facility appear to have been successfully revoked, that user can still perform certain tasks as if the permissions had not been revoked.

Resolution: Fixed

QCCRID 100078

Description: ZIP installation paths - allow special characters in environment variables for Windows x64 versions.

Platform: Windows x64

Subsystem: OCC Client Framework

Symptom: The Windows x64 versions have environment variables for the program file directories which include special characters (parentheses). For example, the environment variable `%ProgramFiles(x86)%` represents the directory `C:\Program Files (x86)`.

SA currently doesn't allow special characters within environment variables when changing the default installation path of ZIP file packages.

Resolution: Fixed

QCCRID 84111

Description: In the Device Group browser, when you select Device Membership and choose the Import option to import servers through a CSV file, you are unable to change focus to another window.

Platform: Independent

Subsystem: OCC Client Framework

Symptom: Entire interface is locked because of the modal dialogue window which prevents users from checking data on other windows.

Resolution: Fixed

Custom Extensions

QCCRID 92622

Description: SA uses the wrong IP address to contact the Core on a system with virtual IPs on same subnet.

Platform: Independent

Subsystem: Custom Extensions (CX) - Single user mode helper

Symptom: In single user mode, a packet to a specific IP address is assigned a different address. Currently, in this situation, SA appears to use DESTINATION GATEWAY NETMASK and, when routes are added, does not consider interfaces.

Resolution: Fixed

Data Access Engine

QCCRID 95875

Description: Remote commands can take too log to initiate in a remote datacenter.

Platform: Independent

Subsystem: Data Access Engine (Spin)

Symptom: Remote commands can take as much as 120 seconds before they are finally initiated on the remote datacenter. Short scripts are also executed in serial instead of in parallel.

Resolution: Fixed

QCCRID 99604

Description: Should support Windows Server 2008 R2 as a managed platform.

Platform: Windows Server 2008 R2

Subsystem: Data Access Engine (Spin)

Symptom: Should support Windows Server 2008 R2 as a managed platform (OS provisioning, compatible agent and patching).

Resolution: Fixed

Gateways

QCCRID 93982

Description: The Gateway (`opswgw`) `chroot` environment on Linux x86_64 is missing the `/lib64` directory.

Platform: Linux

Subsystem: Gateway

Symptom: When the Gateway (`opswgw`) is installed on a Linux x86_64 system, the `/lib64` directory is not created in the `opswgw chroot` environment. This can prevent the gateway from being able to properly egress proxied TCP connections, failing with a name lookup error.

Resolution: Fixed

Global File System

QCCRID 100563

Description: Multiple vnodes pointing to the same inode.

Platform: Independent

Subsystem: Global Filesystem/Shell Backend

Symptom: Intermittent failure in ogfs_forget() caused by two vnodes in OGFS kernel module got mapped to same inode in the hub. This occurs when the directory /opsw/.user is accessed from scoped and unauthenticated sessions. The cause of the failure is identified as the 'tag' used to create unique inode does not take scope into consideration.

Resolution: Fixed

Model Repository

QCCRID 93757

Description: The database user `truth` statistics collection job fails with error: `ORA-01000: maximum open cursors exceeded`.

Platform: Independent

Subsystem: Model Repository (Truth)

Symptom: `ORA-01000: maximum open cursors exceeded - set cursor_sharing = exact (shell script)`

Resolution: Fixed

Networking

QCCRID 92622

Description: System uses the wrong IP address to contact the core on a system with virtual IPs on same subnet.

Platform: Solaris

Subsystem: CX - Single user mode helper

Symptom: System uses wrong IP address to contact core on a system with virtual IPs on same subnet

Resolution: Fixed

OS Provisioning

QCCRID 89237

Description: Provisioning a VMWare ESX 3.5 VM with Windows Server 2008 fails due to permission issues.

Platform: Windows Server 2008/VMWare ESX

Subsystem: OS Provisioning - OCC - client

Symptom: Running a Windows Server 2008 OS Sequence on a VM server Fails with the error message: Results not Found.

Resolution: Fixed

QCCRID 90094

Description: New version of the HP NC-Series Broadcom 1Gb Driver for Windows Server 2003 available

Platform: Windows Server 2003

Subsystem: OS Provisioning - Backend

Symptom: Support needed for the HP NC-Series Broadcom 1Gb driver for Windows Server 2003.

Resolution: Fixed

QCCRID 93128

Description: Re-open an OS Sequence with a pre -/ post-Remediate script that is run as `root`. `Name/Password/Domain` fields become editable.

Platform: Independent

Subsystem: OS Provisioning - OCC - Client

Symptom: Create an OS Sequence with Remediation enabled. Specify a Saved script and to run as root without password. Save the OS Sequence and close the object window. Open the OS Sequence again and go to the Remediation task view. At this point the `Name/Password/Domain` fields and should not be.

Resolution: Fixed

QCCRID 93847

Description: Windows Server 2008 OS provisioning fails due to inability to resolve hostnames.

Platform: Windows Server 2008

Subsystem: OS Provisioning Backend

Symptom: When the client boots WinPE and attempts to mount the media, it cannot, because the client cannot resolve any hostnames.

Resolution: Fixed

QCCRID 95918

Description: The physical memory in a Windows VM created by Microsoft Hyper-V is not correctly determined.

Platform: Independent

Subsystem: OS Provisioning Backend

Symptom: SA does not correctly determine the physical memory in a Windows VM created by Microsoft Hyper-V.

Resolution: Fixed

QCCRID 99603

Description: An OS Provisioning Media Server import fails to import Windows Server 2008 SP2 media.

Platform: Windows Server 2008 SP2

Subsystem: OS Provisioning Backend

Symptom: When attempting to import Windows Server 2008 SP2 media to the OS Provisioning Media Server, you receive an OS detection error and the media fails to import. Windows Server 2008 SP1 media imports successfully.

Resolution: Fixed

Patch Management - Solaris

QCCRID 90961

Description: A Solaris patch policy attached through a Device Group does not display an inherited icon and tooltip.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: When a software policy is attached through a Device Group, on the device's patch policy view, the policy should be shown as inherited from the group (a different icon) and tooltip on mouseover but does not.

Resolution: Fixed

QCCRID 91806

Description: A Solaris patch policy attached through a device group does not show inherited icon and tooltip.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: Solaris patch policies attached through device group do not show inherited icon and tooltip. For both windows patch policy and SW policy, if the policy attached through a device group, on a device's patch policy view, the policy will be shown as inherited from group (different icon) and tooltip when mouse over to this policy. This is not true for Solaris patch policy.

Resolution: Fixed

QCCRID 92173

Description: The DCML Exchange tool (DET/CBT) does not update platform associations for units on second import after an export using the `-incr` argument.

Platform: Independent

Subsystem: Patch Management - Solaris

Symptom: The platform list for a patch in the target core is not updated during a DET import with the `-incr` option.

Resolution: Fixed

QCCRID 92426

Description: A Solaris local zone's Server Browser Installed Patches list does not show a patch that was installed through a Patch Policy remediated at the global zone level.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: Create a patch policy applicable to both local and global zones, attach patch policy only to the global zone and remediate. The server browser does not show patches as installed for the local zone

Resolution: Fixed

QCCRID 93225

Description: Modification of a platform in a Solaris patch policy is not validated against the platforms of the servers attached to the policy.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: Modification of Solaris patch policy platform does not take into account the existing attached server platforms. This can lead to errors in the compliance scan on the server.

Resolution: Fixed

Patch Management - Windows

QCCRID 79697

Description: The Windows Patch Management database incorrectly identifies required patches.

Platform: Windows

Subsystem: Patch Management - Windows

Symptom: Compliance tests can produce a result that disagree with the `Patches Needed` view, and the patch remediation job. This is due to use of the `<software_release>` field of the `RecommendedPatch` record which is a GUID for the Microsoft patch versus the Microsoft Q/KB number.

Resolution: Fixed

QCCRID 83968

Description: When Windows servers with no recommended patches are scanned for addition to an SA Core, they are not moved out of the Scan Needed state.

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: Windows servers with no recommended patches do not move out of Scan Needed state after being scanned for addition to a core.

Resolution: Fixed

QCCRID 90509

Description: Windows patching: Right Click ➤ **Set Availability** doesn't save availability. status

Platform: Windows

Subsystem: Patch Management - Windows - UI

Symptom: Right clicking on a Windows patch and selecting **Set Availability ➤ Available** to set the availability does maintain the selected state.

Resolution: Fixed

QCCRID 92308

Description: Software Policies that contains patches that supersede other patches in the same policy can cause remediation failures.

Platform: Windows

Subsystem: Patch Management - Windows

Symptom: MBSA's metadata does not declare supersedence relationships correctly, or at least how SA expects them to be declared which can cause patches that have been superseded to fail when they are installed in the wrong order.

Resolution: Fixed

QCCRID 93393

Description: A Patch Scan can fail if an exception for a patch exists in a policy attached to a server and the server's device group

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: When you attach a policy to a server, attach the policy to the server's device group, set an exception for the server for a patch in the policy, and then invoke a patch compliance scan on the server, the following error occurs:

```
An error occurred while calculating compliance results. The Command Engine
either was unable to contact the Web Services Data Access Engine (twist) or
the twist returned a generic error.
```

Resolution: Fixed

QCCRID 93496

Description: The timeout for installing a Windows hotfix can be reduced from 60 minutes.

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: A Widows hotfix installation times out after 60 minutes when it should timeout after 10 minutes.

Resolution: Fixed

QCCRID 94132

Description: A Windows server's **Recommended Patches** list may not display certain patches as recommended even though the patches are recommended by the patch scanning engine.

Platform: Windows

Subsystem: Patch Management - Windows - UI

Symptom: The **Recommended Patch** list is missing certain patches even though a patch scan on the managed server showed the patches as needed.

Resolution: Fixed

QCCRID 97792

Description: Reports for Patch Management can have incorrect or mismatched session ID in the compliance summary table.

Platform: Independent

Subsystem: Patch Management - Windows - Backend

Symptom: Reports for Patch Management can have incorrect or mismatched session ID in the compliance summary table.

Resolution: Fixed

Powershell

QCCRID 90201

Description: The Powershell cmdlet fails with the error `Set-SasServer : No such operation 'update'`.

Platform: Windows 2003

Subsystem: Web Services

Symptom: When trying to modify the description of a server using the Powershell cmdlet error appears: `Set-SasServer : No such operation 'update'`

Resolution: Fixed

SA Client

QCCRID 92982

Description: An Advanced Search using the Agent Discovery Date Between rule creates a dynamic group with incorrect date values.

Platform: Independent

Subsystem: Search

Symptom: When the user creates a dynamic server group from Advanced Search results using `Agent Discovery Date Between Date1 AND Date2`, the rule is changed to `Between Date1-minus-1-day AND Date1`.

Resolution: Fixed

QCCRID 93159

Description: A query on the Job Table does not return the correct results when a job ID is specified in the filter.

Platform: Independent

Subsystem: Search

Symptom: The query on the job table is not returning the right results when a job ID is specified in the filter.

Resolution: Fixed

QCCRID 94277

Description: URL for the deployed web services is invalid.

Platform: Independent

Subsystem: Web Services

Symptom: All deployed web services are displayed as being at *https://<hostname>/ws4ee/services*. This link stopped working in 7.8, works on pre 7.8 cores.

Resolution: Fixed

SAS Web Client

QCCRID 70583 (159229)

Description: Random user actions sometimes cause `HTTP Status 500` in the SA Web Client.

Platform: Independent

Subsystem: SAS Web Client

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

Resolution: Fixed

Scripts

QCCRID 82714

Description: Script output to export is limited to 10Kb, need a textbox in UI to allow flexible output size.

Platform: Independent

Subsystem: DSE (UI)

Symptom: The script output size is limited to 10K. When output > 100K, the script output is truncated because of the UI limitation.

Resolution: Fixed

Server Module

QCCRID 83143

Description: Improved error message required when the file `tadnsw.exe` is missing.

Platform: Independent

Subsystem: Server Module - Discovery Modules

Symptom: When `tadnsw.exe` is from a managed server and a snapshot specifications run, a stack trace is shown with a message that does not specify the name of the missing file.

Resolution: Fixed

QCCRID 92829

Description: A snapshot for the software discovery inventory fails on HP-UX with the error `unknown encoding: iso88591`.

Platform: Independent

Subsystem: Server Module - Backend

Symptom: Running a snapshot for the software discovery inventory fails on some HP-UX servers with the error:

```
OpswareError: serverCompliance.FailedToCreateSnapshot [ module:
com.opsware.compliance.server.rmi, method: createSnapshot, line: 219

[...]
```

Resolution: Fixed

QCCRID 93173

Description: SMO-registered software displays fewer items compared to the installed packages list for Red Hat 64-bit since some packages have both 32- and 64-bit versions but both versions are displayed as a single item.

Platform: Red Hat Enterprise Linux

Subsystem: Server Module - Packages and Patches

Symptom: Red Hat packages that have both 32- and 64-bit versions may incorrectly display as a single package in the SMO-registered software display.

Resolution: Fixed

QCCRID 94119

Description: Running a snapshot with the `Perform Inventory` option on VMWare ESX servers, an error occurs indicating that the database installation appears to be corrupted.

Platform: ESX

Subsystem: Server Module - Discovery Modules

Symptom: Running a snapshot with the `Perform Inventory` option on VMWare ESX servers, an error occurs indicating that the database installation appears to be corrupted.

Resolution: Fixed

QCCRID 95403

Description: SMOs should allow values to be added/changed for certain audit parameters, for example, `Account Lockout Threshold`.

Platform: Independent

Subsystem: Server Module - Backend

Symptom: Some SMOs have integer display maps but don't allow the user to input values that are not in the map.

Resolution: Fixed

QCCRID 99173

Description: Non-compliant audit results in the Details window are labeled with the wrong color (blue instead of red) and Java console errors occur.

Platform: Independent

Subsystem: Server Module - Backend

Symptom: Non-compliant audit results in the Details window are labeled with the wrong color (blue instead of red) and Java console errors occur.

Resolution: Fixed

Software Management

QCCRID 72251

Description: When running remediate for a software policy containing a package the package is not installed.

Platform: Independent

Subsystem: Software Management - Backend - Remediate (Other)

Symptom: Remediate job completes with the message:

```
This software install was attempted and appeared successful, but after
verification, Opsware determined that it was not actually installed.
```

Resolution: Fixed

QCCRID 76594

Description: Should allow triggering reboots immediately after running a script in a software policy.

Platform: Independent

Subsystem: Software Management - Backend - Remediate (Other)

Symptom: During complex software policy remediations, the user needs the ability to include a reboot during the installation process. Specifically, the ability to reboot after running a script which is not currently supported.

Resolution: Fixed

QCCRID 88615

Description: Remediate should handle RPM dependencies more intelligently when remediating detached software policies.

Platform: Linux

Subsystem: Software Management - Backend - Remediate (RPM packages)

Symptom: Since RPM dependencies are now taken into account during remediation, it possible for a user to effectively `rm -rf /` a managed server. The reason for this is that when removing an RPM, remediate also removes everything that depends upon that RPM.

For example, a customer creates a policy with a single RPM, `glibc`. They remediate, and thus SA adopts this package. They change their mind, detach the policy, and remediate again.

At this point, the dependency solver adds essentially every other RPM on the server to the remove list since almost everything depends on `glibc`.

Resolution: Fixed

QCCRID 90586

Description: Improve error message when an Application Installation Media (AIM) install script exits with non-zero exit code.

Platform: Independent

Subsystem: Software Management - UI - Install/Uninstall/Remediate

Symptom: A "`Warning: could not remove the following extracted files/directories`" message masks the actual third-party application error when the Install script of an Application Installation Media (AIM) package exits with a non-zero exit code. In the case where there is no error message from the third-party application installer other than the return code, it is not clear to the end user what caused the installation to fail.

Resolution: Fixed

QCCRID 93309

Description: After an ad hoc User Group installation, if the user group name does not follow Solaris naming conventions, the job status shows as Not Installed even though the user group has been installed.

Platform: Solaris

Subsystem: Software Management - Backend - Remediate (Other)

Symptom: The final job status shows the user group as not installed but it is installed/created on the server.

Resolution: Fixed

QCCRID 94127

Description: Software policy remediation attempts to install Windows user/group object on a Solaris server and fails.

Platform: Solaris

Subsystem: Software Management - Backend - Remediate (Other)

Symptom: If the platform of an object is not applicable to a server, remediation should filter out such object in preview. In the following case, software policy remediation attempts to install Windows user/group object on Solaris server and fails.

Resolution: Fixed

QCCRID 94379

Description: Application Configuration provisioning hangs.

Platform: Independent

Subsystem: Software Management - Backend - Remediate (Other)

Symptom: Running a large number of application configurations can cause an intermittent hang during provisioning and the provisioning job shows `Completed with Errors`.

Resolution: Fixed

QCCRID 96839

Description: Software compliance is always shown as Non-compliant if there is application configuration in the Software Policy.

Platform: Independent

Subsystem: Software Management - API - Compliance

Symptom: Software compliance is always shown as Non-compliant if there is an application configuration in the Software Policy.

Resolution: Fixed

QCCRID 97790

Description: Reports for Software Management can have incorrect or mismatched session ID and Compliance Summary data.

Platform: Independent

Subsystem: Software Management - API - Software Policy

Symptom: Reports for Software Management can have incorrect or mismatched session ID and Compliance Summary data.

Resolution: Fixed

QCCRID 100395

Description: Software Compliance does not work correctly when there are two RPMs with the same name but different versions on the same server.

Platform: Linux

Subsystem: Software Management - API - Compliance

Symptom: Software Compliance does not work correctly when there are two RPMs with the same name but different versions on the same server.

Resolution: Fixed

QCCRID 100396

Description: Software Compliance does not work correctly on x86_64 platforms.

Platform: x86_64 platforms

Subsystem: Software Management - API - Compliance

Symptom: Software Compliance does not work correctly on x86_64 platforms.

Resolution: Fixed

QCCRID 100417

Description: When there are old and new versions of the same RPM on a server, RPMs with versions in between are marked as not compliant.

Platform: Independent

Subsystem: Software Management - API - Compliance

Symptom: When a server has rpm-1.0, rpm-2.0, and rpm-3.0 installed, rpm-2.0, is marked as not compliant.It should be marked compliant.

Resolution: Fixed

QCCRID 100854

Description: Continue on Errors option does not work when remediating a Software Policy with an application configuration.

Platform: Independent

Subsystem: Software Management - Backend - Remediate (Other)

Symptom: Continue on Errors option does not work when remediating a Software Policy with an application configuration.

Resolution: Fixed

Virtualization

QCCRID 83067

Description: Agent for VMWare ESX 4 does not read the RAM size as expected.

Platform: VMware

Subsystem: Virtualization - Backend (VMWare)

Symptom: For ESX 4, the agent does not read the RAM size.

Resolution: Fixed

QCCRID 89739

Description: Create or Modify VM not working for non-ASCII characters in the name/description.

Platform: VMWare

Subsystem: Virtualization - Backend (VMWare)

Symptom: After creating a VM with Japanese characters in the name and description, the hypervisor history shows that the VM was created and displays the Japanese characters correctly. However, the VI client, does not display the characters correctly.

If you create the VM from the VI client itself, using Japanese characters, they display correctly in both the UI and VI client.

Resolution: Fixed

QCCRID 93055

Description: In the Server Browser, the Hyper-V periodical scan history is incorrectly referred to as a VMWare ESX scan.

Platform: Microsoft Hyper-V

Subsystem: Virtualization - Microsoft Hyper-V

Symptom: `Scanning the ESX periodically for local Virtual machines` is displayed in the Server Browser history of a Hyper-V server when a periodic Hyper-V scan occurs.

Resolution: Fixed

QCCRID 93123

Description: When creating a VM with an old job window open, the Create VM job fails with error stating the VM name already exists.

Platform: VMWare

Subsystem: Virtualization - UI

Symptom: While running a `Create VM` job you open the an old job ID from the Jobs and Sessions list.You now have two windows open: the create VM window and the old job window. If you click on start job in the Create VM window, it fails with the above error.

Resolution: Fixed

QCCRID 93220

Description: After discovering a VMWare ESX VM, a virtual server refresh generates the Java console exception: `AWT-EventQueue-0"`
`java.lang.ArrayIndexOutOfBoundsException: 14 > 13`.

Platform: ESX

Subsystem: Virtualization - UI

Symptom: After discovering the VMWare ESX server, a scan is performed (ESX ➤ Virtual Servers > Refresh) and this generates the following exception in java console.

```
Exception in thread "AWT-EventQueue-0"
java.lang.ArrayIndexOutOfBoundsException: 14 > 13
```

Resolution: Fixed

QCCRID 93589

Description: Cannot change the size of disk being added to a VM in a powered-on state.

Platform: Independent

Subsystem: Virtualization - UI

Symptom: When modifying a VM, if the VM is in a powered-on state, you can add a disk but cannot change the size of the new disk nor change the datastore once one is selected.

Resolution: Fixed

QCCRID 93703

Description: Attempting to create a virtual machine (VM) and provision an OS on a virtual machine without installing a network interface (NIC), SA creates multiple VMs until it runs out of resources.

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

Symptom: If you attempt to create a virtual machine (VM) and provision an OS on a virtual machine without installing a network interface, SA creates multiple VMs until it runs out of resources.

Resolution: Fixed

QCCRID 93756

Description: In a Solaris 10 hypervisor History view, a recurring scan event is not logged.

Platform: Solaris

Subsystem: Virtualization - Backend (Zones)

Symptom: In the History view of a Solaris 10 hypervisor, recurring scan event is not logged.

Resolution: Fixed

QCCRID 94076

Description: Creating or modifying multiple VMs at nearly the same time fails on VMWare ESX and ESXi.

Platform: ESX & ESXi

Subsystem: Virtualization - Backend (VMWare)

Symptom: Open a few create VM windows from the same hypervisor and change some data in each. All VMs are created with the same name, even when different names are specified in each window.

Resolution: Fixed

QCCRID 94207

Description: VMWare ESX 3.5 feature Open Console does not work.

Platform: VMWare ESX 3.5

Subsystem: Virtualization - Backend (VMWare)

Symptom: For VMWare ESX 3.5, right click a VM, and select the Open Console feature. This loads a page where user can login, but then issues the message: `Web service is unavailable`.

Resolution: Fixed

Visual Analyzer

QCCRID 84313

Description: When a Windows Server 2008 server with an IIS role enabled is visualized, it is shown as an unconnected process.

Platform: Windows 2008

Subsystem: Visual Analyzer - UI

Symptom: When you visualize a Windows Server 2008 server with an IIS role enabled, the IIS process is shown in the unconnected processes box instead of it's own process box on the server map.

Resolution: Fixed

Web Services Data Access Engine

QCCRID 83222

Description: Conflict resolution operations should have smaller impact on performance.

Platform: Independent

Subsystem: Web Services Data Access Engine (Spin)

Symptom: Internal changes to improve performance required.

Resolution: Fixed

QCCRID 92819

Description: The Web Services Data Access Engine (twist) consumes 100% CPU.

Platform: Independent

Subsystem: Web Services Data Access Engine (twist)

Symptom: Web Services Data Access Engine (twist) is consuming 100% cpu.

Resolution: Fixed.

4 Known Problems, Restrictions, and Workarounds in SA 7.81

The issues in this section are identified by their Quality Center ID (QCCRID).

For information regarding open issues for SA Storage Visibility and Automation and the Server Automation Reporter (SAR), please refer to the *Release Notes* for those products.

Agents

QCCRID 100660

Description: Windows ADT login fails for administrators that are not user `Administrator`.

Platform: Windows Server 2008 using UAC

Subsystem: Windows Agent Deployment

Symptom: On Windows Server 2008, Windows ADT login fails for administrators that are not user `Administrator` due to Windows UAC security controls.

Workaround: Turn off UAC:

1. In the Control Panel, click User Accounts.
2. In the User Accounts window, click User Accounts.
3. In the User Accounts tasks window, click Turn User Account Control on or off.
4. If UAC is currently configured in Admin Approval Mode, the User Account Control message appears. Click Continue.
5. Clear the Use User Account Control (UAC) to help protect your computer check box, and then click OK.
6. Click Restart Now to apply the change right away, or click Restart Later and close the User Accounts tasks window.

After the workaround is performed, any user belonging to the Administrators group will be able to deploy agents.

QCCRID 102401

Description: Duplicate MAC addresses for certain devices prevent the agent from installing and prevent hardware registration.

Platform: All

Subsystem: Agent Deployment or Hardware Registration

Symptom: An error message like the following occurs when installing an agent or during a hardware registration:

```
ERROR: spin.notUniqueInDatabase - More than one Server found with interface
 hw_addr '33:50:6F:45:30:30'
```

Workaround: This error occurs because certain devices use duplicate MAC addresses, such as WAN Miniports. SA can detect some of these devices. However, if you have a device not detected by SA, you need to add the following line to the file `/etc/opt/opsware/spin/spin.args` on all your core servers where the Data Access Engine (spin) is running and append your new MAC address to this list.

```
spin.device.ms_dup_macs: ['50:50:54:50:30:30', '33:50:6F:45:30:30',
 '00:00:00:00:00:00', '02:00:4C:4F:4F:50']
```

For example, if you received the following error:

```
ERROR: spin.notUniqueInDatabase - More than one Server found with interface
   hw_addr '02:00:00:00:00:00'
```

You would need to add the following line to the file `/etc/opt/opsware/spin/spin.args` on your core servers:

```
spin.device.ms_dup_macs: ['50:50:54:50:30:30', '33:50:6F:45:30:30',
 '00:00:00:00:00:00', '02:00:4C:4F:4F:50', '02:00:00:00:00:00']
```

After modifying this file on all core servers where the Data Access Engine (spin) is running, restart the Data Access Engine on all those core servers.

Audit and Compliance

QCCRID 102706

Description: After a patch rollback, Compliance Dashboard pick lists are empty on Secondary Cores running SA 7.81 when the First Core is version 7.80.

Platform: Independent

Subsystem: Audit and Compliance

Symptom: After a patch rollback, audits, patches and AppConfig, software policies are missing from the Select Compliance Columns dialog on an SA 7.81 Secondary Core if the First Core is SA 7.80.

Workaround: The pick lists are empty because the search to fill them relies on a new SA 7.81 search field that is not in the database because of the rollback. In a Multi-master mesh, HP recommends that you patch the primary core first, followed by secondary cores and satellites, thus ensuring that the primary core is at a higher version (such as SA 7.81 or higher) than the secondary cores. If you must roll back the SA 7.81 patch in a Multi-master Mesh, HP recommends that you roll back the secondary cores and satellites first, then the primary core.

However, if you cannot rollback a scondary core(s), you can restore the missing data by running the following on the 7.81 secondary core(s):

```
/opt/opsware/bin/python2 /var/opt/opsware/OPSWpatch/OPSWspin/scripts/
QC94469_apply.pyc
```

Global File System

QCCRID 93497

Description: Solaris core only, all `ttlg` runs terminate due to lack of swap space.

Platform: Solaris

Subsystem: Global File System/Shell Backend

Symptom: Solaris core only, all `ttlg` runs terminate due to lack of swap space.

Workarounds:

- Increase the swap space configured for the system (recommended)
- Reduce the swap usage for the system.

Hyper-V

QCCRID 97630

Description: In a multi-master mesh environment, simultaneous invocations of scheduled periodic scans on hypervisors can cause multi-master conflicts. These scheduled periodic scans on hypervisors are triggered by the SA user “virt_scanner”.

Platform: Windows

Subsystem: Hyper-V

Symptom: Multi-master conflicts occur.

Workaround: Use the multi-master tools to resolve these conflicts.

QCCRID 98310

Description: If your Hyper-V server has more than one IP address, SA may change the Management IP address from the one you registered to one of the other IP addresses.

Platform: Windows

Subsystem: Hyper-V

Symptom: SA may change the Management IP address from the one you registered to one of the other IP addresses.

Workaround: Edit the Windows server's TCP/IP hosts file, located at %Windir%\system32\drivers\etc\hosts and add a line of the form:

<IP-address> <FQDN>

Where *<IP-address>* is the Management IP address and *<FQDN>* is the fully qualified domain name of the server as displayed in the “Name” column of the SA Client. For example:

```
192.168.158.3 k003.hypervqa.hp.com
```

QCCRID 101449

Description: Hyper-V operations are not supported in some environments running both SA 7.80 and 7.81.

Platform: Windows

Subsystem: Hyper-V

Symptom: If you have a multimaster mesh and if your primary core is running SA 7.80 and one or more secondary cores are running SA 7.81, then SA will manage Hyper-V VMs, but operations to create, modify and delete VMs are not supported.

Workaround: Install SA7.81 on all the cores in your multimaster mesh. As an alternative, if your primary core is running SA 7.81 and one or more secondary cores are running SA 7.80, then most Hyper-V operations are supported provided you run the SA Client from a 7.81 core. Creating and provisioning Hyper-V VMs is supported only if your Hyper-V server is registered to a SA 7.81 core and you run the SA Client from a 7.81 core.

QCCRID 102344

Description: The Hyper-V operations to create, modify and delete a VM are not supported if your Hyper-V server is registered to a core running SA 7.80.

Platform: Windows

Subsystem: Hyper-V

Symptom: If you have a multimaster mesh and if your Hyper-V server is registered to a core running SA 7.80, then the Hyper-V operations to create, modify and delete VMs are not supported.

Workaround: Install SA 7.81 on all cores in your multimaster mesh. As an alternative, if your primary core is running SA7.81, all Hyper-V operations are supported for servers registered to the primary core and installed with a 7.81 agent.

Installer

QCCRID 100931

Description: Patch upgrade reports `"Failed to remove software policy 'Storage Compliance Checks' (8710001)" structures must start and end within the same entity`.

Platform: Independent

Subsystem: SA Installer

Symptom: While performing a rollback of the SA 7.81 patch, the following console error occurs and is stored in the correspondent log file under /var/log/opsware/opsware_installer:

```
Removing com.opsware.server.module.storage.compliance
This will probably take a long time.
[...]
Failed to remove ServerModule from servers
[…]
```

```
Failed to remove software policy 'Storage Compliance Checks' (8710001)
ProtocolError: <ProtocolError for 192.168.161.22/cogrpc.py: 404 Not found>
```

The rollback fails to remove Storage Compliance, which is new in 7.81 and not compatible with SA 7.80. After reporting the error, rollback continues to the next component. The rollback completes successfully without other errors and cleans up all patch-related files and folders on the core.

Workaround: Manually remove Storage Compliance by running the following command on one of core servers:

```
/opt/opsware/bin/smtool --username=detuser --password=<detuserpwd>
--remove=com.opsware.server.module.storage.compliance
```

Model Repository

QCCRID 93757

Description: ORA-01000: maximum open cursors exceeded - set cursor_sharing = exact (shell script).

Platform: Independent

Subsystem: Model Repository/Oracle RDBMS 11.1.0.7

Symptom: In some cases, the database user `TRUTH` statistics collection job fails with the error: `ORA-01000: maximum open cursors exceeded`. This error is intermittent and not all customers will experience this issue. The error is caused by an Oracle bug (#7651092). When this error occurs, you may see entries similar to the following in Oracle's `alert.log` file:

```
<timestamp>
Errors in file /u01/app/oracle/diag/rdbms/truth/truth/trace/<filename>.trc:
ORA-12012: error on auto execute of job 1
ORA-01000: maximum open cursors exceeded
ORA-06512: at "SYS.DBMS_STATS", line 18566
ORA-06512: at "SYS.DBMS_STATS", line 19051
ORA-06512: at "SYS.DBMS_STATS", line 19132
ORA-06512: at "SYS.DBMS_STATS", line 19088
ORA-06512: at line
```

Workaround: With SA 7.81, a script is provided that modifies the TRUTH database user's `dba_job` that collects the schema statistics. Perform the following tasks to apply this workaround:

Copying the Script

The scripts, `modify_truth_stats_job.sh` and `modify_truth_stats_job.sql`, are found in the directory:

```
/opsware_installer/tools/truth_modify_stats_job
```

Copy the scripts to any directory on your Model Repository (`truth`) host, for example,

```
/var/tmp/modify_truth_stats_job.sh
/var/tmp/modify_truth_stats_job.sql
```

Running the Script

The following is required to run the script:

- You must run the script as root

You will also need the following information:

- ORACLE_HOME
- ORACLE_SID
- Password for the schema owner TRUTH

Script usage

`./modify_truth_stats_job.sh <oracle_home> <oracle_sid>`

For example:

```
./modify_truth_stats_job.sh /u01/app/oracle/product/11.1.0/db_1 truth
```

QCCRID 96568

Description: Cannot duplicate a zip package.

Platform: Independent

Subsystem: Model Repository - Truth

Symptom: When duplicating a zip package, the package is duplicated without the path and the following error message is displayed:

`You do not have permission to view details of this policy item.`

Workaround: You must run a shell script as described below:

`truth_unit_folder_trigs.sh`

The `truth_unit_folder_trigs.sh` script calls the `truth_unit_folder_trigs.sql` script which modifies two triggers in the Model Repository schema:

- `UNIT_SHADOW_FLDR_AS_RTRG` on the `UNIT_RELATIONSHIPS` table
- `FLD_UNIT_SHADOW_FLD_UNIT_RTRG` on the `FOLDER_UNIT` table

After modifying the triggers, the script processes any unprocessed data in `SHADOW_FOLDER_UNIT` table.

First, copy the following files from the SA 7.81 distribution to any directory on the Model Repository host:

- `/opsware_installer/tools/truth_unit_folder_trigs.sh`
- `/opsware_installer/tools/truth_unit_folder_trigs.sql`

For example:

```
/var/tmp/truth_unit_folder_trigs.s*
```

Before you run the script, you must have the following information available:

- `ORACLE_HOME`
- `ORACLE_SID`
- The password for schema owner `TRUTH`

To run the script, log on to the Model Repository host as `root` and invoke the script:

```
# ./truth_unit_folder_trigs.sh <oracle_home> <oracle_sid>
```

For example:

```
./truth_unit_folder_trigs.sh /u01/app/oracle/product/11.1.0/db_1 truth
```

When the operation is complete, you will see the following message

```
Task completed
```

Rollback

If you need to rollback the modifications made to the triggers, you can run the following scripts:

- `truth_unit_folder_trigs_rollback.sh`
- `truth_unit_folder_trigs_rollback.sql`

First, copy the files from the SA 7.81 distribution to any directory on the Model Repository host, for example:

```
/var/tmp/truth_unit_folder_trigs_rollback.s*
```

Before you run the script, you must have the following information available:

- `ORACLE_HOME`
- `ORACLE_SID`
- The password for schema owner `TRUTH`

To run the script, log on to the Model Repository host as `root` and invoke the script:

```
# ./truth_unit_folder_trigs_rollback.sh <oracle_home> <oracle_sid>
```

For example:

```
./truth_unit_folder_trigs_rollback.sh /u01/app/oracle/product/11.1.0/
db_1 truth
```

When the operation is complete, you will see the following message

```
Task completed.
```

OS Provisioning

QCCRID 93849

Description: Linux reprovisioning becomes interactive if the value for `truth.dcNm` is not the same as the value for `truth.dcDispNm`, or `truth.dcDispNm` is not specified in uppercase only.

Platform: Linux

Subsystem: OS Provisioning - Reprovisioning

Symptom: In a core where the value for `truth.dcNm` is not the same as the value for `truth.dcDispNm`, or `truth.dcDispNm` is not specified in uppercase only, Linux reprovisioning becomes interactive and prompts the user for the language, locale, etc.

Both the`truth.dcNm` and `truth.dcDispNm` parameters were set during core installation.

Workaround: None

QCCRID 101920

Description: Solaris 10 packages are only partially installed.

Platform: Solaris

Subsystem: OS Provisioning Backend

Symptom: Solaris 10 SPARC OS Provisioning job completes with the status `Success`, however the output in the client shows a `Solaris 10 packages partially installed` message.

Workaround: Copy the file:

`Solaris_10/Tools/Boot/X_small.cpio.bz2`

from your Solaris 10 boot media, into the directory:

`/opt/opsware/boot/jumpstart/Boot/boot`

QCCRID 102449

Description: Using the SA `ProductKey` custom attribute to provide the Windows Server 2008 R2 volume license key information leads to an invalid product key error.

Platform: Windows Server 2008 R2

Subsystem: OS Provisioning Backend

Symptom: If you attempt to specify the Windows Server 2008 R2 volume license product key information by using the SA `ProductKey` custom attribute for Windows 2008 R2 OS Provisioning, the Windows setup process fails with the following error

```
The unattended answer file contains an invalid product key. Either remove the
invalid key or provide a valid product key in the unattended answer file to
proceed with Windows Installation.
```

Workaround:

- *Do not* specify the Windows Server 2008 R2 volume license product key information by using the SA `ProductKey` custom attribute during OS Provisioning.
- Ensure that the SA `ProductKey value` *is not* specified in the `unattended.xml` file's `<settings pass="windowsPE">` section.
- Ensure that the `ProductKey` value is provided in the `<settings pass="specialize">` section, `Microsoft-Windows-Shell-Setup` component, of the `unattended.xml` file.

QCCRID 102830

Description: Cannot enter a timeout value for pre/post remediate scripts while creating a new OS Sequence.

Platform: Independent

Subsystem: OS Provisioning - OCC - client

Symptom: When you are creating a new OS Sequence, the timeout value pre/post remediate scripts cannot be modified.

Workaround: None

Permissions

QCCRID 101710

Description: Clone Server Permission is obsolete.

Platform: Independent

Subsystem: Permissions, Server Management

Symptom: The permissions reference in the *SA Administration Guide* incorrectly lists a permission for an obsolete feature: `Clone Server`.

Workaround: None. The Clone server permission should be ignored.

Satellites

QCCRID 97659

Description: Network scans to a satellite realm fail for hosts with the error: `XML document structures must start and end within the same entity`.

Platform: Windows

Subsystem: Satellites

Symptom: Network scans fail with an error.

Workaround: In the SA Client Options select **Tools ➤ Options ➤ Unmanaged Servers ➤ Advanced** and remove the argument `-S %GATEWAY_IP%` from the NMAP parameters.The network scan should complete successfully.

Software Management

QCCRID 100754

Description: You cannot set the time-out value for the time it takes to install or remove software or execute scripts to anything other than the default value of 5 hours. This time-out value is specified by “way.remediate.action_timeout” in the SAS Web Client.

Platform: All

Subsystem: Software Management

Symptom: If a job to install or remove software or to execute a script takes longer than 5 hours and you set the time-out value to greater than 5 hours, the job still times out after 5 hours. If you set the time-out value to less than 5 hours, the time-out still occurs after 5 hours.

The job fails with the message "The request to retrieve information from the Agent failed because it timed out. If the problem persists, please contact your HP Server Automation Administrator."

You set the time-out value for jobs that install or remove software or execute scripts from the SAS Web Client under "System Configuration" -> "Command Engine" -> "way.remediate.action_timeout". Any value you set for "way.remediate.action_timeout" is not recognized. The default value of 5 hours (18,000 seconds) is always used. This means that jobs will time out if the action (the time it takes to install or remove software or execute scripts) takes longer than 5 hours regardless of the value set for "way.remediate.action_timeout".

Workaround: None

QCCRID 101517

Description: After performing a software remediation, the compliance status may not be accurate. This is because of a caching delay in the Web Services Data Access Engine (twist).

Platform: All

Subsystem: Software Management

Symptom: After performing a software remediation, the compliance status may incorrectly show servers out of compliance.

Workaround: Run a Software Policy Compliance scan. This will show the correct compliance status. For more information, see "Software Compliance" and "The Software Policy Compliance Scan" in the *SA User Guide: Application Automation*.

QCCRID 102109

Description: Remediation of software and patch polices fails on Linux platforms.

Platform: Linux

Subsystem: Software Management - Backend - Remediate (RPM packages)

Symptom: When attempting to remediate a Linux server, the operation fails with an error such as:

```
The remediate operation cannot be performed because an error occurred during
preview.
/var/opt/opsware/yum/cache/opsware/repomd.xml:9: parser error
```

Workaround: This error can be caused by the root environment containing any `*_proxy` environment variables such as `http_proxy` and `https_proxy`. Remove these variables from the root environment, then restart the agent and try the operation again. It is recommended that the server be rebooted to ensure the variables have been properly removed.

QCCRID 102564

Description: Software Compliance scan status is `Scan Failed` after attaching and remediating a software policy.

Platform: Solaris

Subsystem: Software Management - API - Compliance

Symptom:

1. Attach a software policy to a Solaris server.
2. Perform a software compliance scan (right-click a Managed Server and select **Scan Software Compliance**).
3. Remediate.
4. Perform a software compliance scan (right-click managed server and select **Scan Software Compliance**).

   A `Scan Failed` message is displayed for steps 2 and 4.

This error occurs when the file `solpatchdb.zip` (the solaris metadata database) is missing.

Workaround: Use `solpatch_import` to create the metadata database. See the Patch Management for Solaris in the *SA User Guide: Application Automation* for more information about `solpatch_import`.

Software Repository

QCCRID 99828

Description: A cascading satellite (an SA satellite whose gateway is connected to another satellite's gateway rather than to an SA Core Management Gateway) cannot connect to the Software Repository cache of another satellite due to a certificate error.

Platform: Independent

Subsystem: Software Repository

Symptom: When you attempt Agent Deployment on an unmanaged server from a cascading satellite, the operation fails with the error: `Agent Binary staging failure`.

Workaround: Do not cascade the satellite gateways, connect the satellite gateways directly to a Core Management Gateway.

Solaris Patching

QCCRID 95745

Description: When resolving the dependencies for a set of Solaris patches in a patch policy, the incompatible patches dialog may repeatedly be displayed. This can occur when an incompatible patch is required by another patch in the patch policy or when an incompatible

patch obsoletes another patch in the patch policy. After you specify an incompatible patch to be removed from the policy, it may get added back because it is required by some other patch in the policy, resulting in the incompatible patches dialog being redisplayed.

Platform: Solaris

Subsystem: Solaris Patching

Symptom: The incompatible patches dialog is repeatedly displayed because of a set of patches with a chain of dependencies that causes the incompatible patch to be added back into the patch policy.

Workaround: When the incompatible patches dialog is displayed, choose a different patch. Or remove from the patch policy all the patches that require or are obsoleted by the incompatible patch that you want removed.

For more information, see "Patch Management for Solaris" in the *SA User Guide: Application Automation*.

QCCRID 98409

Description: When importing a Solaris patch cluster into the SA Library, sometimes the vendor documentation for the cluster is not imported.

Platform: Solaris

Subsystem: Solaris Patching

Symptom: Vendor documentation is not present when viewing the cluster in the SA Client. However, a link to the vendor documentation is provided.

Workaround: Select the link to the vendor documentation and log in to the Sun web site. Select the link again to download the cluster documentation.

QCCRID 100566

Description: The reboot setting for the last patch in a Solaris patch policy may be displayed incorrectly, even though the reboot is performed correctly.

Platform: Solaris

Subsystem: Solaris Patching

Symptom: When you preview remediating a Solaris patch policy on a server or when you view the job status for a Solaris patch policy that has already been remediated, the last patch may incorrectly show "Install and Reboot Later" as the reboot setting when it should show "Install and Reboot."

Workaround: None needed because the reboot is performed correctly even though the display may be incorrect.

QCCRID 101449

Description: The Resolve Dependencies operation in the SA Client is not supported in some environments running both SA 7.80 and 7.81.

Platform: Solaris

Subsystem: Solaris Patching

Symptom: If you have a multimaster mesh and if your primary core is running SA 7.80 and one or more secondary cores are running SA 7.81, and you select the Solaris patching Resolve Dependencies button or menu item in the SA Client, it will fail.

Workaround: Install SA 7.81 on all the cores in your multimaster mesh. As an alternative, if your primary core is running SA 7.81 and one or more secondary cores are running SA 7.80, then the Resolve Dependencies operation is supported provided you run the SA Client from a 7.81 core.

VMware ESX4 Hypervisor Console

QCCRID 93492

Description: If the vmware-webAccess service is not running, you cannot open the VMware console from SA.

Platform: VMware

Subsystem: VMware Console

Symptom: Attempting to open the VMware console from a VMware virtual machine fails if the “vmware-webAccess” service is not running on the hypervisor.

To open the VMware console, select a VMware virtual machine and select the **Actions** menu or right click and select **VMware Virtual Machines ➤ Open Console...**

Workaround: To check if this service is running, run the following command:

```
# /etc/init.d/vmware-webAccess status
```

To start the service if it is not running, run the following command:

```
# /etc/init.d/vmware-webAccess start
```

5 Documentation Errata

This chapter contains additional information that affects the SA 7.80 product manuals.

SA Planning and Installation Guide

The following changes should be applied to the *SA Planning and Installation Guide*.

Chapter 1: SA Core Component Bundling (page 15)

The sentence in the first paragraph that reads:

During a Custom installation, certain components can be broken out of their bundles (such as the Command Engine, the OS Provisioning Boot Server and Media Server, among others) and installed on separate servers.

should read:

During a Custom installation, certain components can be broken out of their bundles (such as the Software Repository Store, Slice Component bundle, OS Provisioning Media Server, OS Provisioning Boot Server etc.) and installed on separate servers.

Chapter 3: Solaris Requirements (page 48)

In **Table 11**: Packages Required for Solaris, the packages marked with double asterisks indicating them as required for Solaris 8 or 9 should be ignored as Solaris 8 and 9 are not supported.

Chapter 3: Pre-Installation Requirements, Table 18 (page 59)

Table 18 in the SA Planning and Installation Guide correctly lists port 1521 as required to be open in your firewall configuration. However, the following information can also affect your firewall configuration:

- Port 1521 is the default Oracle listener (`listener.ora`) port, but you can specify a different port in your Oracle configuration. In case your installation has been modified to use a port other than 1521, you should verify the port number from the Oracle listener status and ensure that your firewall is configured to allow the correct port to be open for the Oracle listener.
- SA's data access layers (infrastructure) use connection pooling to the database. The connections between the database and the infrastructure layer must be maintained as long as SA is up and running. Ensure that your firewall is configured so that these connections do not time-out and terminate the connections between the database and the infrastructure layers.

Appendix A: Table 42 (Page 188)

In **Table** 42: Supported Operating Systems and Oracle Versions, the first entry, SunOS 10 x86_64, should read, SunOS 10 (SPARC)-64 bit.

Appendix A: Solaris Requirements (page 190)

In the bulleted entry that reads:

- Free `/tmp` space should be 400MB or more

  You can use the following command to check `/tmp` space:

  ```
  df -k /tmp | grep / | awk '{ print $3 }'
  ```

  the command should read:

  ```
  df -k /tmp | grep / | awk '{ print $4 }'
  ```

Appendix A: Required and Suggested Parameters for init.ora (page 203)

The following `init.ora` parameters should have the specified required values:

Both Oracle 10g and 11g

```
optimizer_mode=all_rows
session_cached_cursors>=50
```

Oracle 10g only

```
open_cursors>=300
remote_login_passwordfile=EXCLUSIVE
```

Oracle 11g only

```
open_cursors>=1000
memory_target=1616M
```

SA Upgrade Guide

Chapter 1: OS Provisioning Stage 2 Image Upload No Longer Required (page 8)

The sentence that reads:

However, due to this change, any Satellites in an SA 7.80 Core must also be upgraded to release 7.80 in order to provision servers. In other words an SA 7.80 Satellite can perform OS Provisioning in an SA 7.80 Core but an SA 7.50 Satellite cannot.

is not valid. You can perform OS Provisioning in a mixed version SA Core/Satellite environment.

Chapter 3: Phase 1, Step 3b (page 46)

This step should read:

Select `Multimaster Opsware Core - Subsequent Core`

Chapter 3: Phase 6 (page 50)

A step is missing after Step 3:

Step 4 Log on to the Slice Component bundle host, select `Slice` from the Upgrade Component menu. Press c to continue.

The existing Step 4 should be renumbered Step 5.