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: 9.0

Release Notes

Document Release Date: June 2010
Software Release Date: June 2010

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

Copyright Notices

Trademark Notices

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://h20230.www2.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	Version	Changes
1. What's New in SA 9.0	9.0	Updated for SA 9.0 new features.
2. Platform and Environment Support for SA 9.0	9.0	Updated for SA 9.0.
3. What's Fixed in SA 9.0	9.0	Added descriptions for bugs fixed for SA 9.0.
4. Known Problems, Restrictions, and Workarounds in SA 9.0	9.0	Added descriptions for bugs that are known problems in SA 9.0.
5. Documentation Errata	9.0	Added updates to SA 9.0 product documentation.

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 What's New in SA 9.0

HP Server Automation (SA) 9.0 automates critical areas of server and application operations—including provisioning, patching, server and application configuration change management, virtual server management, compliance checking and reporting—across major operating systems and a wide range of software infrastructure and applications.

This chapter describes all new features and enhancements in the SA 9.0 release.

The SA 9.0 release also includes bug fixes, enhancements, and features in the SA 7.81 release. However, the Virtuozzo feature provided in the SA 7.81 release is not available in the SA 9.0 release. See the *SA 7.81 Release Notes* for more information.

SA 9.0 excludes bug fixes, enhancements, and features in the SA 7.82 and SA 7.83 releases. Subsequent 9.x releases will incorporate bug fixes, enhancements, and features in the SA 7.82 release, SA 7.83 release, and so on. For more information, contact HP Software Support or review the release notes for specific product versions.

➤ As with previous SA releases, all SA Core installations and upgrades must be performed by HP Professional Services or HP-certified consultants. SA Satellite installations and upgrades performed by customers continue to be supported.

➤ For information regarding new features for the HP Storage Visibility and Automation and BSA Essentials, see the *Release Notes* for those products.

New & Improved Documentation

To improve the retrievability and usability of SA product documentation, several new documentation components were added in this release, such as Quick Start video clips and an interactive HTML documentation list.

To improve and expand the SA documentation library architecture, several new PDF guides were also added in this release. See the notations in Documentation PDF Library on page 12.

Quick Start Videos

In this release, short video clips that quickly show you how to use HP Server Automation have been added to the online Help.

Watch the Quick Start Videos

To view the Quick Start videos, from the SA Client, select the Help menu and then select Contents and Index. This displays the SA online Help. Select *Quick Start with Server Automation* and then select any topic in the list. Click the video icon ▶ to watch the video.

Download the Latest Quick Start Videos

You can download the latest version of *Quick Start with Server Automation* by going to the HP Software Product Manuals web site at:

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

Log in with your HP Passport or register and request an HP Passport. On the HP Software Product Manuals web site, select the following:

- **Product**: HP Server Automation
- **Version**: 9.0 (or later)
- **Operating System**: Select any operating system
- Click **Search**.

This site displays all available HP Server Automation manuals and online Help, including the latest version of *Quick Start with Server Automation*.

Interactive HTML Documentation List

The SA HTML Documentation List is a handy interactive master list of the SA documentation set. It lists all of the documents provided with each SA release, a brief description of the document's content and direct links to the document PDFs that can be opened in a browser or saved locally and opened using a PDF reader. It also contains links to the HP Self Solve manuals download site and HP support pages. You can access the HTML Documentation List from the SA Documentation DVD, install it on a documentation host or incorporate it into an internal SA information web site or Wiki.

Documentation PDF Library

For this release, the following HP Server Automation documentation is available for this release. These documents are in PDF format.

To check for updates, 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, select the **New users - please register** link on the HP Passport login page.

- *SA Release Notes*
- *SA Overview and Architecture Guide* (New!)
- *SA Single-Host Installation Guide* (New!)
- *SA Simple/Advanced Installation Guide* (New!)
- *SA Upgrade Guide*
- *SA Support Matrix*
- *SA Quick Reference: SA Installation*
- *SA Oracle Setup for the Model Repository*
- *SA Administration Guide*
- *SA Integration Guide* (New!)
- *SA Content Utilities Guide*
- *SA Content Migration Guide*
- *SA Platform Developer Guide*
- *SA Policy Setter Guide*
- *SA Application Configuration User Guide* (New!)
- *SA Application Deployment User Guide* (New!)
- *SA User Guide: Server Automation*
- *SA User Guide: Application Automation*
- *SA 9.0 and BSA Essentials 2.0 Reports*
- *Storage Visibility and Automation Release Notes*
- *Storage Visibility and Automation Installation & Administration Guide*
- *Storage Visibility and Automation Upgrade Guide*
- *Storage Visibility and Automation Support Matrix*
- *Storage Visibility and Automation User Guide*
- *Storage Compliance User Guide*
- *Storage Reports User Guide*
- *SE Connector Installation Guide*
- *SE Connector Release Notes*

New Application Deployment Manager

Applications can be complex to deploy—they need to be deployed more and more frequently, and they have become critical to company success. When deployed manually, lower application quality and higher life cycle costs often result. SA now automates deploying your custom applications throughout the application life cycle (Development to QA to Staging to Production) so that you can deploy your custom applications consistently, at lower cost, and with higher quality.

See the *SA Application Deployment User Guide* for instructions on how to deploy your custom applications.

New Application Deployment Reports

For additional information about these reports, refer to the *SA and BSA Essentials Reports Guide*.

Application Deployment Activity Reports

This report provides a list of all Application Deployment actions that are performed within a specified time range along with the details related to these actions.

ROI Reports

The ROI reports enable you to see the Return On Investment (ROI) that you are realizing by using Application Deployment. You can generate a report grouped by Application or by Environment.

Deployment Success Reports

These reports enable you to view data that describes how often Application Deployments succeed. For each month in the selected date range, the report shows you the number of deployment jobs that were attempted and the number that were successful.

Time to Production Reports

The Time To Production reports enable you to see how long it takes for your applications to work their way through the application lifecycle. For each release of an application, the report shows how long it took for the application to reach the last stage in the application lifecycle (typically the Production environment).

Installation

As with previous SA releases, all SA Core installations and upgrades must be performed by HP Professional Services or HP-certified consultants. SA Satellite installations and upgrades performed by customers continue to be supported.

Simplified Installation

SA 9.0 provides new, simplified installation methods. There are now four installation methods:

- **Single Host, Local Model Repository**: This method can be used to install all SA Core components, including the required HP-supplied Oracle database, on a single host to manage servers in a single facility. You need only provide values for three configuration parameters

  For more information, see the *SA Single-Host Installation Guide*.

- **Simple Installation**: The Simple Installation allows you to distribute SA core components to different hosts and allows a remote Model Repository.
- **Advanced Installation**: This method also allows a remote Oracle database for the Model Repository, including SA core components distributed to different hosts, and provides more granular control of configurable paths and integrations.
- **Expert Installation**: Typically used for complex enterprise SA Core installations and for troubleshooting installation problems.

  For more information, see the *SA Simple/Advanced Installation Guide*.

Installation Prerequisite Checking

During installation, SA 9.0 automatically checks your host environment to ensure that it meets SA 9.0 requirements and recommended configuration.

You can also run this check as a standalone utility prior to installation to verify the suitability of a server as an SA Core host before attempting an installation.

The prerequisites that are validated during the check include:

- **Oracle Database** - diskspace, parameter, tablespace requirements (*existing Oracle installations only*)
  - Supported Oracle version is installed
  - Required operating system packages and patches are installed
- **Required Packages** - packages that must be installed
- **Required Patches** - patches that must be installed (SunOS only)
- **Recommended Packages** - packages that should be installed
- **Unsupported Packages** - packages that must not be installed
- **Diskspace Requirements** - checks that minimum diskspace required for installation available (*fresh installation only*)
- **Physical attributes**:
  - Memory
  - Number of CPUs
- **Operating System Configuration**:
  - Hostname is a fully qualified domain name (FQDN) and is resolvable
  - Allocated swap space
  - Timezone setting
  - Appropriate locales are available
  - Sufficient `temp` space is available
  - Translations for localhost are available
  - System runlevel verification
  - Verification that no critical file paths contain symbolic links

Easier Searching and Filtering of Job Results

In SA 9.0, Advanced Search has been enhanced so that you can search for jobs that affect certain managed servers or device groups.

Filtering job types (such as Audit Servers, Deploy Application, Remediate Policies, and so on) was added so that you can customize what displays in the Job Status pane. This enables you to easily and quickly find key information about your jobs. You can filter, group, sort, search for, and highlight information in the detailed job results. You can expand or narrow the detailed job results, depending on what information you want displayed or hidden.

See the *SA User Guide: Server Automation* for instructions on how to perform an advanced search and how to customize your job results display.

See also the short video that demonstrates some of the new searching and filtering capabilities. From the SA Client, select the Help menu and select Contents and Index. This displays the SA online help. Select the topic Quick Start with Server Automation and select Searching Job Results. Select the video icon to view the video.

Application Configuration Improvements

Application configurations and templates have been moved into SA Library folders, similar to most of the server automation artifacts. This makes managing your application configurations much simpler and more consistent with other processes. The configuration template editor also adds syntax highlighting and color coding for easier editing of configuration templates. For complete details, see the *SA Application Configuration User Guide*.

See Deprecated API Methods on page 22.

Server Automation-Operations Orchestration Content

The Operations Orchestration (OO) SA integration allows administrators to build OO flows that are integrated with HP Server Automation (SA).

See the *Operations Orchestration Implementation Guide* for installation and configuration instructions, operation parameters and tools, use-case scenarios, sample OO flows, and information about troubleshooting and securing your system.

Virtual Server Management

VMware Virtual Machine Cloning

In SA 9.0, you can clone a virtual machine. When you clone an existing virtual machine, you create a copy of the source virtual machine. HP Server Automation provides several key benefits that add business value when you clone an SA-managed virtual server. The cloning process enables you to create a new virtual machine that:

- SA can manage, patch, and configure.

- Is compliant with your operating system patch levels.
- Inherits the identical SA management model, whose compliance status you can manage.

  The management model consists of the following items:

  - Custom Attributes
  - Custom Fields
  - Installed Software
  - Installed Packages
  - Application Configuration Instances
  - Static Device Group Associations
  - Snapshot Specification Associations
  - Audit Policy Associations
  - Windows Patch Policy Associations
  - Solaris Patch Policy Associations
  - Software Policy Associations

See the *SA User Guide: Server Automation* for instructions on how to clone a VMware machine.

Registering Virtualization Services

HP Server Automation manages **Virtualization Services** (VS) such as **VMware vCenter Server.** VMware vCenter provides a scalable and extensible platform that centrally manages hypervisors and virtual machines (vm). With SA you can manage the hypervisors and virtual machines under Virtualization Services. You need to register Virtualization Services in SA, at which point SA connects to the VS and brings all the hypervisors under SA management. For more information and instructions on how to register a Virtualization Service, see “Virtualization Service Management” in the *SA User Guide: Server Automation*.

Patch Management for Windows

Patching Compliance Evaluates Superseded Patches (Windows OS Service Packs)

In the previous SA release, a patch policy's compliance calculation did not account for those patches on the server that have been superseded. In this release, Windows patching compliance will consider a server's patch status as non-compliant if a superseded patch in a policy is not installed on a server attached to the policy.

Patch Install Preview, Job Details, and Notification Enhancement

In this release, when you run the patch install or patch remediate task wizard, the Preview step now displays explanations for those patches that will not be installed due to a variety of reasons. For example, if the patch policy contains an exception that indicates a patch should never be installed (Never Install), the patch will be called out in the dialog with an explanation.

Patch Policy Window Now Shows Superseded Patches

In the Patch Policy Window ➤ Policy Items view, if the policy contains a patch that is superseded by another patch (a more recent version exists), the user interface now indicates each patch that has been superseded.

Windows Server 2008 R2 Support

SA now supports Windows Patching on Windows Server 2008 R2 for both .exe and .cab file formats.

New Windows Patching Reports

Time to Patch Compliance

This new report shows you how long it takes (the average number of days) for your Windows servers to become compliant after a Windows patch policy change.

When a change is made to a Windows patch policy (patch added), then the server or servers that the policy is attached to is considered non-compliant until the server is remediated to match the patch policy definition.

ROI: Servers Affected by Windows Patch Policy Updates

This new report shows you the ROI of remediating Windows patch policies using HP Server Automation.

OS Provisioning

OS Build Plans

As of this SA release, OS Provisioning provides support for a new, more flexible method for Windows hosts to specify how an operating system is installed called *OS Build Plans*. You use an OS Build Plan to specify server provisioning details, such as operating system configuration information, software, customization scripts and patch policies.

➤ SA provides a set of baseline OS Build Plans that you copy and use to base your Build Plans on. These Build Plans are not installed by default during SA installation or upgrade, rather you will be required to download the plans from BSA Essentials and install them using the DCML (DET) tool. Instructions for installing the baseline OS Build Plans are included with the download.

While similar to the OS Sequence capability, OS Build Plans provide these functional improvements over OS Sequences:

- OS Build Plans make it easier to customize the operating system installation to meet your specific needs, for example:
  - Integration with other internal systems at specific points during the operating system build phase.
  - Running a RAID configuration utility or a firmware update
  - Modifying the unattend.xml file from a script before beginning an installation process
- Simpler architecture. OS Build Plans use the same network ports and protocols as a full SA Agent. Fewer SA Core Components are involved.
- OS Build Plans use the more robust and powerful execution environment of the Global Shell (OGFS).
- A more transparent build process means easier progress monitoring and troubleshooting.
- The use of an OGFS Agent provides an easy way to configure and troubleshoot servers before or during an operating system build.
- OS Build Plans allow simpler set up:
  - Running the `import_media` utility is no longer required.
  - Defining OS Installation Profiles in the SAS Web Client is now optional, not required.
- No separate client installation is required to deploy operating systems.
  - The new Run OS Build Plan wizard is a web application.
  - The SA Client can be used to define OS Build Plans.
  - Build Plan APXs can be run from the command line or from scripts.
- Perform other tasks beyond OS Installation. For example, OS Build Plans can be created for image capture, file restore, or secure data erasure.

➤ You can still use OS Sequences to configure your Windows operating system installation. The functionality is still fully available. See the *SA User's Guide: Application Automation*. HP recommends, however, that you explore the advanced features of OS Build Plans and consider migrating from OS Sequences to OS Build Plans. OS Build Plans are currently available only for Windows operating system installations.

Booting Servers in a Non-DHCP Environment

You can use OS Provisioning in an environment without a DHCP server. You can assign static IP information for the managed server and manually configure that server to resolve the SA Core.

Supported operating systems are:

- Red Hat Enterprise Linux x86 and x86_64

- Red Hat Enterprise Linux Itanium Server x86_64
- Windows Server 2003 and 2008

There are several reasons you might need to manually specify the network information for a sever being provisioned:

• You don't use DHCP and must manually specify the static IP address the Agent's IP and Port

• You must provision a server but DHCP is inactive.

• You must provision a server but DHCP is blocked by firewall rules.

For more information, see the *SA User's Guide: Application Automation*.

HP RAID Support

You can configure disk mirroring and striping as part of the initial setup of an HP server prior to provisioning an operating system.

HP RAID configuration requires having an HP server configured with a baseline RAID configuration that is captured to a software policy.

For more information, see the *SA Policy Setter Guide*.

Multimaster Master Gateway Backup Routes

With this SA release installation of a third core and subsequent cores in a Multimaster Mesh by default automatically creates backup routes between the cores' Master Gateways.

For example, for a three core or greater mesh, all Multimaster traffic is routed as usual through the First Core's Master Gateway. However, the Second Core's Master Gateway is now designated, by default, as the backup Master Gateway to be used should the First Core's Master Gateway fail. All additional subsequent cores' Master Gateways added to the mesh will be designated as backups in the order of installation. To support backup routes, third and subsequent cores will by default have two tunnels. The first tunnel communicates with the First Core's Master Gateway, the second tunnel with the Second Core in the mesh.

For more information, see the *SA Overview and Architecture Guide*.

BSA Essentials Installation

BSA Essentials is now installed as part of the SA Core installation.

➤ BSA Essentials is not supported under Red Hat Linux AS3.

LDAP Authentication Configuration Tool

The LDAP Authentication Configuration tool allows you to import both LDAP users and user groups into the SA Model Repository. This tool can be run from the command line or by selecting and running the LDAP Authentication Configuration tool from the SA Client APX Library.

Predefined User Groups

During a fresh installation of SA, certain predefined user groups are created with default privileges based on roles. Use of the predefined user groups is optional. You can change the privileges of the predefined user groups; you can also delete these groups. Changes or deletions of the predefined user groups are not affected by SA upgrades. Some of the predefined user groups are:

- System Administrators
- Superusers
- Viewers
- OS Policy Setters
- OS Deployers
- Patch Policy Setters
- Patch Policy Deployers
- Software Policy Setters
- Software Policy Deployers
- and more...

See the *SA Administration Guide* for more information about predefined user groups.

Showing the Progress of an APX

SA adds the `apxprogress` command which you can use in your program APXs to provide information about the progress of your APX. This is useful for program APXs that run for a long period of time when you want to give the user status on the progress of your APX. For details, see the *SA Platform Developer Guide*.

Deprecated Features

When a feature or platform is identified as *deprecated* for a release, it means that you (the SA customer) are notified of its future removal. Deprecated features are still fully supported in the release they are deprecated in, unless specified otherwise. The intent is that deprecated features or platforms will have support removed in the next major or minor SA release; however, eventual removal is at the discretion of HP.

The following features were deprecated in the SA 7.80 release. Current and future availability of these features is also described in the following sections:

Deprecated API Methods

In SA 9.0, moving application configurations and configuration templates into folders changed the behavior of the associated classes and services.

Attributes folder and lifecycle of the VO-s are required for the following API calls:

```
com.opsware.acm.ConfigurationService#create
com.opsware.acm.ConfigurationService#update
com.opsware.acm.CMLService#create
com.opsware.acm.CMLService#update
```

The following methods have been deprecated, but they still perform as expected. Method `com.opsware.folder.FolderVO#getCustomers` should be used instead.

```
com.opsware.acm.ConfigurationVO#getCustomers
com.opsware.acm.CMLVO#getCustomers
```

The following methods have been deprecated and they have a void implementation. `Method com.opsware.folder.FolderVO#setCustomers` must be used instead.

```
com.opsware.acm.ConfigurationVO#setCustomers
com.opsware.acm.CMLVO#setCustomers
```

Code Deployment and Rollback (CDR) and Configuration Tracking

Code Deployment and Rollback (CDR) was deprecated in the SA 7.80 release, but is still supported in SA 9.0. In a future release, this feature will not be supported. The new Application Deployment tool in SA 9.0 is intended to replace CDR. See New Application Deployment Manager on page 13 and the *SA Application Deployment User Guide* for more information.

For more information about the deprecation of CDR, contact your HP Technical Support representative.

Agent Deprecation

In SA 9.0, HP is announcing the deprecation of the Server Automation Agent for the following versions:

- Server Automation 7.01
- Server Automation 7.00
- Server Automation 6.xx
- Server Automation 5.xx

Although releases of HP Server Automationprior to 9.0 will continue to support these versions of the Agent, it is recommended that customers migrate to newer versions of the Agent on their managed platforms.

HP SA will stop supporting these versions of the Agent in an upcoming major or minor release. Agents from Server Automation 4.xx and earlier are not supported in this release.

DOS-Based OS Provisioning

DOS-based OS Provisioning was deprecated in the SA 7.80 release and is not supported in SA 9.0. For more information, contact your HP Technical Support representative.

start_opsware.sh and stop_opsware.sh scripts

Previous versions of SA provided the following start and stop scripts:

```
start_opsware.sh
stop_opsware.sh
```

As of SA 7.80, these scripts are no longer supported.

In SA 9.0, you must use the unified start script:

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

If you have any applications or scripts that depend on this script, you must rewrite them to use the unified start script.

Virtual Server Management Actions

The Open Console action (for VMware virtual machines of ESX agent-managed hypervisor) was removed in this release.

The Open Web Access action (for ESX agent-managed hypervisors) was removed in this release.

Virtualization actions for agent-managed ESX 3.0 hypervisors are no longer supported, unless the ESX 3.0 hypervisor is managed by a Virtualization Service. It cannot be directly added to the Virtual Servers view (through Add Hypervisor); it needs to be vCenter managed.

2 Platform and Environment Support for SA 9.0

Supported Operating Systems for Server Automation 9.0

See the *SA Supported Platforms* document for a detailed list of supported operating systems for SA Cores, Managed Servers, Agents, Satellites, and clients. This document is located in the documentation directory of your SA installation.

3 What’s Fixed in SA 9.0

Agents

QCCR1D: 70222

Description: Windows agents do not update their `opswgw.args` file.

Platform: Windows

Subsystem: Agents

Symptom: In certain cases, when gateways are added to a Multimaster Mesh, the existing Agents are not refreshing their list of gateways correctly.

Resolution: Fixed.

QCCR1D: 74021

Description: The agent installer should detect when it is communicating with a new core.

Platform: Independent

Subsystem: Agent Installer

Symptom: In certain cases, when a new core is installed on a server with an existing Server Agent, the Agent may not be uninstalled during the new core installation, leaving the Agent’s existing crypto information that will not match with the crypto information for the new core. In this case, the existing Agent communication with the new core will fail.

Resolution: Fixed.

QCCR1D: 74339

Description: Remove SSLv2 handshake from the Agent.

Platform: Independent

Subsystem: Agents

Symptom: For a secure environment, SSL v2 handshaking should be removed from the SA Agent. SSLv3 is supported.

Resolution: Fixed.

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'
```

Resolution: Fixed.

Audit and Remediation

QCCR1D: 55465

Description: It should be possible to flag Windows Registry audits as non-case sensitive.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: Windows registry audits are currently case sensitive. This can lead to many false positives where keys are considered different when they only differ in case.

Resolution: Fixed.

QCCR1D: 69863

Description: Large audits can cause the Web Services Data Access Engine (`twist`) to crash.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: Audits that have several hundred thousand audit results can cause the Web Services Data Access Engine (twist) to crash.

Resolution: Fixed.

QCCR1D: 89044

Description: An audit with a large number of servers fails with an out-of-memory exception.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: An audit run on a large number of servers (+150) may not complete successfully due to memory issues.

Resolution: Fixed.

QCCR1D: 92932

Description: Snapshot specification job fails with a legacy exception on a Windows XP server.

Platform: Windows

Subsystem: Audit and Compliance Backend

Symptom: Snapshot specification jobs can fail with the following legacy exception on Windows XP server:

Summary: An error occurred during the audit.

```
Detail: An error occurred during the audit.
Resolution Steps: Please see the additional messages for more information. If
this does not resolve the issue, contact your Opsware administrator. Legacy
Error Code: wayscripts.auditGenericError msg= All member snapshots in a
Snapshot template failed.
```

Resolution: Fixed.

Command Engine

QCCR1D: 71848

Description: The Command Engine (waybot) does not properly handle failure to start PENDING jobs when the Command Engine is available again.

Platform: Independent

Subsystem: Command Engine

Symptom: If the Command Engine is too busy or otherwise unavailable, PENDING jobs cannot be run, however, when the Command Engine is available again, the missed PENDING jobs run, regardless of how old they might be.

Resolution: Fixed.

PENDING jobs now have a default limit of 600 seconds after which they are considered stale jobs and will not be run when the Command Engine becomes available again. (This limit is configurable but you must contact your SA Support Representative to change the default time.) For example, you have a one-time job that is scheduled to run at a future date and time. When it is time for the job to run, the Command Engine is down. When the Command Engine comes back up, the PENDING jobs are inspected, to check whether or not the job should run based on when the job was scheduled versus the current time, and if too much time has passed (600 seconds by default), the job is not run.

Custom Fields

QCCR1D: 70320

Description: Searching for servers by custom fields sometimes returns incorrect results.

Platform: Independent

Subsystem: Custom Fields - Search

Symptom: Searching for servers using custom fields as search parameters in the SA Client, the SAS Web Client, and the Command Center browser can return invalid results due to incorrect filtering.

Resolution: Fixed.

Data Access Engine

QCCR1D: 67030

Description: The Data Access Engine (`spin`) cannot handle more than 1024 connections (Too many files open errors).

Platform: Independent

Subsystem: Data Access Engine

Symptom: When the Data Access Engine exceeds 1024 connections, too many files open errors occur. The connection limit for the Data Access Engine should be increased to 65536.

Resolution: Fixed.

DCML Export Tool (DET)

QCCR1D: 91664

Description: DET exports all account-based ValueSets for each Application Configuration associated with an account.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: DET should export only the ValueSets associated with an Account, instead it exports all ValueSets included those of associated customers.

Resolution: Fixed.

QCCR1D: 92144

Description: Import of OS Sequences sets the wrong values, causing software remediation to fail.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: Import of OS Sequences populates incorrect flags in certain fields. Therefore, after OS Provisioning completes, software remediation jobs do not start and the build fails.

Resolution: Fixed.

Global File System

QCCR1D: 58417

Description: Umount fails because of reference count bug in kernel module.

Platform: Solaris

Subsystem: Global File System/Shell Backend

Symptom: The Global File System (OGFS) cannot be stopped properly because it cannot be unmounted and the host must be rebooted before the OGFS can be started again.

Resolution: Fixed.

Microsoft 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.

Resolution: Fixed.

ISM Tool

QCCR1D: 71625

Description: The command `cat loginToServer` fails with an Input/Output error.

Platform: Independent

Subsystem: Global Shell/Shell UI

Symptom: When a customer, facility, or device group is deleted, all resource settings on either a user group or an OGFS privilege which references that object should also be removed. When they are not, the command `cat loginToServer` fails with an Input/Output error.

Resolution: Fixed.

QCCR1D: 92201

Description: During ISM software remediation, the control config script sets environment variables incorrectly.

Platform: Windows

Subsystem: ISM Tool

Symptom: When using the ISM tool to build and upload an ISM package on a Windows managed server (using the ZIP package engine) and a configuration control script for access to custom attributes, the environment variables `ISMLIB` and I`SMRUNTIMEDIR` are not set to the correct paths.

Resolution: Fixed.

Model Repository

QCCR1D: 91064

Description: Oracle Setup for the Model Repository does not list required Oracle patches.

Platform: Independent

Subsystem: Model Repository

Symptom: Oracle (10g) setup for the Model Repository requires that certain Oracle patches also be installed. These patches are installed automatically during an HP-supplied Oracle database installation. However, the patches must be manually supplied if you are using the Oracle Universal Installer to install the database or are using an existing Oracle 10g database.

Resolution: Fixed.

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
```

Resolution: Run the standalone shell script from `/opsware_installer/tools/truth_modify_stats_job` from the SA distribution.

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.
```

Resolution: Fixed.

OS Provisioning

QCCR1D: 71989

Description: Remediation with pre/post scripts fails during Linux Provisioning.

Platform: Linux

Subsystem: OS Provisioning - Backend

Symptom: During Linux OS provisioning using a Software Policy and remediate pre-action and post-action scripts, the job fails when the Pre-Action script runs. All further Remediation steps are skipped and do not complete.

Resolution: Fixed.

QCCR1D: 88820

Description: Samba version must be upgraded due to issues about securing the environment with the shipped version.

Platform: Linux

Subsystem: OS Provisioning - Backend

Symptom: The version of the Samba server installed on the remote host during Linux OS provisioning has problems with securing the environment and should be upgraded to a secure release.

Resolution: Fixed.

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.

Resolution: Fixed.

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.

Resolution: Fixed.

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.
```

Resolution: Fixed.

Patch Management for Solaris

QCCRID: 95745

Description: 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.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: 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.

Resolution: Fixed.

Patch Management for Windows

QCCR1D: 82708

Description: GB Locale not mapped to the Microsoft Patch DB

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: If your system locale is set to GB (0809), Microsoft Windows patches are not displayed correctly in the SAS Web Client.

Resolution: Fixed.

Software Management

QCCR1D: 74750

Description: Remediate fails with `KeyError: next_phase_args` error.

Platform: Independent

Subsystem: Software Management - Backend - Remediate (other)

Symptom: A race conditions occurs during certain remediation jobs requiring retries and multiple remediate attempts.

Resolution: Fixed.

QCCR1D: 83256

Description: CBT does not import changes to a software policy when importing incremental.

Platform: Independent

Subsystem: Software Management - Tools - Migration

Symptom: In some cases, an incremental CBT import of an application policy that adds application configurations to the policy does not import the changes.

Resolution: Fixed.

QCCR1D: 83916

Description: An incorrect error message is displayed during Preview/Remediation when there is insufficient disk space under the /var directory.

Platform: Independent

Subsystem: Software Management - Backend - Remediate (other)

Symptom: During Preview/Remediate, when there is insufficient disk space under /var directory, the following error should display:

```
insufficient disk space
```

However, this error is actually displayed:

```
The request to retrieve information from the Opsware Agent failed for an
unknown reason, please contact your Opsware Administrator.Execution error:
Traceback (innermost last):
File "./base/wayfuncs.py", line 133, in evaluator
File "<string>", line 1212, in ?
File "<string>", line 1174, in main
File "<string>", line 586, in installPCA
File "<string>", line 382, in findTmpdir
AttributeError: debug
```

Resolution: Fixed.

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
```

Resolution: Fixed.

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`.

Resolution: Fixed.

SSL - Secure Environment

QCCR1D: 83898

Description: SSL Null Cipher is presented on port 1028 (`opeproxy`).

Platform: Independent

Subsystem: SSL - Secure Environment

Symptom: A scan on port 1028 found the following issue: "SSL Server Allows Cleartext Communication (NULL Cipher Support) This host is running an SSL server that supports NULL cipher. The NULL cipher is a 0-bit SSL connection that does not provide encryption; any network traffic is in plain text. Solution: Disable the NULL cipher. Reconfigure the SSL server to provide suitable encryption."

Resolution: Fixed.

Virtualization

QCCR1D: 80218

Description: Zone information requests with more than 2GB of memory are not handled correctly by the Web Services Data Access Engine (`twist`).

Platform: Solaris

Subsystem: Virtualization

Symptom: When more than 2 GB memory is allocated for Local Zones, requests for memory information causes Web Services Data Access Engine errors.

Resolution: Fixed.

QCCR1D: 83717

Description: Windows Server 2008 and Red Hat Enterprise Linux 5 cannot be used to create a
VMware VM.

Platform: Windows Server 2008/Red Hat Enterprise Linux 5

Subsystem: Virtualization - Backend (VMWare)

Symptom: The Create Virtual Machine wizard, does not allow creating VMs with Windows Server2008 or Red Hat Enterprise Linux 5.

Resolution: Fixed.

Web Services Data Access Engine

QCCR1D: 60634

Description: The twistOverrides.conf file is truncated when encrypting a password.

Platform: Independent

Subsystem: Web Services Data Access Engine

Symptom: In certain cases, for example, moving a `twistOverrides.conf` file from one core to another that has different encrypted key material, the operation fails and the `twistOverrides.conf` file is truncated.

Resolution: Changes to changes to the `twistOverrides.conf` file are now written to a temporary file and the original is only overwritten on successful completion of an operation.

QCCR1D: 72100

Description: `opsware-sas init` specifies a `$JAVA_HOME` in `/etc/profile` that points to an SA-incompatible Java version.

Platform: Independent

Subsystem: Web Services Data Access Engine

Symptom: If `$JAVA_HOME` is empty, SA will use the Java version installed in `/etc/opt/opsware/j2sdk14/j2sdk14` which typically contains the SA-supplied Java version. However, if you have installed a different Java version or have installed an application that overwrites the Java version in that directory, you could have incompatibility problems.

Resolution: Fixed.

4 Known Problems, Restrictions, and Workarounds in SA 9.0

The issues in this section are identified both by their legacy BUG ID number (when available) and/or their Quality Center ID (QCCR1D).

➤ 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.

Agent Installer

QCCR1D: 107917

Description: Installing the SA agent on Windows platforms sometimes fails.

Platform: Windows

Subsystem: Agent Installer

Symptom: The SA agent fails to install on the Windows server. When the agent installation fails, if you examine the agent log file at `%SystemDrive%\Windows\System32\opsware-agent-installer-<date>.log`, you will see lines referring to “gencache.py”.

Workaround: Remove all the files from the following three directories, if they exist, and reinstall the agent.

```
%SystemDrive%\Program Files\opsware\agent\lcpython15\Lib\site-packages\win32c
om\gen_py\

%TEMP%\gen_py

%SystemDrive%:\Windows\temp\gen_p
```

QCCR1D: 111593

Description: The Agent log indicates that the Agent installation succeeded; however, the Agent was not installed.

Platform: Windows

Subsystem: Agent Installer

Symptom: The Agent fails to install when there is a gateway problem. However, agent_install erroneously reports that the “HP SA Agent Installed successfully”.

Workaround: Make sure the gateway can be reached from the managed server.

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 controls used to secure the environment.

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.

QCCR1D: 110347

Description: If you perform a fresh install of SA 9.0 (as opposed to performing an upgrade from a previous version of SA to 9.0) and you register any Windows servers that are running pre-9.0 agents, those Windows servers will not be able to perform a software scan. This is because certain pre-9.0 Windows patching utilities are no longer used by SA and are not installed on a freshly installed 9.0 core.

If you perform an upgrade from a previous version of SA to SA 9.0, the Windows utilities are retained on the upgraded 9.0 core so the software scans work properly.

Platform: Windows

Subsystem: Agent

Symptom: Windows servers running a pre-9.0 agent will not be able to perform a software scan from a freshly installed SA 9.0 core.

Workaround: After registering your Windows servers with SA 9.0, upgrade the agent on those managed Windows servers. For information on agents, see “Agent Management” in the *SA User’s Guide: Server Automation*.

Application Configuration

QCCRID: 111765

Description: Unable to modify Application Configuration value sets for all scopes (Configuration, Facility, Customers).

Platform: Independent

Subsystem: Application Configuration

Symptom: You have Read or None privileges for Client Feature - Manage Installed Configuration and Backup Servers, and Read-Write privilege for Application Configuration, and you are not able to edit value sets in the Application Configuration browser.

Workaround: Grant Read-Write privilege for Client Features - Manage Installed Configuration and Backups on Servers.

Application Deployment Manager

QCCRID: 110220

Description: Delta Release Code Components do not remove stale files.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When using a FileSystem Code Component in a Delta Release for an Application, the Delta Release will not be able to pick up file deletion changes. File modifications and file additions will be picked up.

Workaround: None. You can choose to use a Script component to delete no longer needed files when deploying Delta Release.

QCCRID: 110637

Description: Package Component file import unreliable for files that are larger than 100MB.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When creating ADM Package Components, large files may not upload successfully using the “Import Package” feature. You may see an error message similar to:

```
Failed to upload installer.msi
(sent 238547 of419232 bytes).
IO Error: #2038
```

Workaround: Increasing the memory available to the SA Client should allow for files up to 350MB to be uploaded using Application Deployment Manager. Larger files can be uploaded using the **Actions ➤ Import Software** menu when editing a package in the Software Library. To increase memory available to the SA Client, modify the “max-heap-size” parameter in `/opt/opsware/occclient/jnlp.tmpl`. For example:

```
<j2se version="1.6" initial-heap-size="128m" max-heap-size="1350m"/>
```

Note that max-heap-size can be adjusted up to ~1350MB for the 32-bit JVM used by the SA Client.

QCCRID: 111106

Description: Problems exporting ADM Environment to Device Group

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When exporting an environment, you receive the following error message:

“java.lang.RuntimeException: Unable to update the device group representing the target '[target name]': DeviceGroup or Server deleted during operation, try again.”

Workaround: Edit the target specified in the error message and remove all servers that have been deleted from the inventory. Export the environment again.

QCCRID: 111656

Description: Timeout before backup/rollback completes for code components.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Backup or rollback steps fail. The message depends on the type of managed servers.

For Unix servers, the message is “script failed with exit code 15.”

For Windows Servers, the message is “script failed with exit code 1,223.”

Workaround: The timeout for rollback and backup scripts is not directly configurable; however, the default time for scripts to run can be modified using this process:

1. Edit the `/etc/opt/opsware/twist/twist.conf` file.
2. Change `twist.serverscript.defaultTimeout=60` to a larger timeout value. The value is in seconds.
3. Restart the Web Services Data Access Engine (twist) using `/etc/init.d/opsware-sas restart twist`.

   Warning: When the Web Services Data Access Engine (twist) is restarted, Server Automation must be idle. Problems will occur if Server Automation is not idle during the restart process.

QCCRID: 111680

Description: Windows backup script may copy files into multiple places and create spurious duplicates.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: On Windows servers, Code components do not properly backup or restore content. Multiple file copies are made during backup and, during rollback, files are restored to the wrong location.

Workaround: This issue is contained entirely within the Windows Code Backup and Windows Code Rollback scripts. These scripts can be accessed and updated within Script Administration by any user with appropriate privileges. After the scripts are updated, they will be applied to any application that references them when a new version of the application is created. Updated scripts are available upon request.

QCCRID: 111959

Description: Multiple OO Flows in an Application cause parameter values mix-ups.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When deploying a Version of an ADM Application that uses multiple OO Flow Components, the flows fail unexpectedly and the ADM log files show that incorrect parameter values are being used. For example, a numeric TCP port identifier is used as the username for connecting to an Oracle database. You will also notice parameters that do not match those originally entered after switching between the different OO Flow Components.

Workaround: Use a single OO Flow Component per ADM Application which calls multiple flows itself (if possible) or a different ADM component type. Contact HP Support for hotfix availability.

QCCRID: 112013

Description: Parameter Editor sets incorrect parameter values when Targets are not uniquely named.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When attempting to set the value of an application parameter differently across your Environments and/or Targets, incorrect table headers appear (such as, a QA Target is presented as belonging to Production) and the new value is stored and displayed incorrectly—the most recently added Target, often incorrectly, is modified and the new value erroneously appears in all columns.

Workaround: Use unique Target names across all Application Deployment Manager environments.

Audit and Remediation

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 secondary 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
```

QCCR1D: 111682

Description: The View button and Contents panel are not displayed for the Rule “Application Configurations” in the Snapshot Specification window.

Platform: Independent

Subsystem: Audit & Compliance

Symptom: The View button and Contents panel are not displayed for the “Application Configurations” rule in the Snapshot Specification window. You cannot add an application configuration rule for the snapshot.

Workaround: Create the audit rule in an audit policy.

BSA Essentials Dataminer

QCCR1D: 112784

Description: In multimaster environments, there is a potential mismatch of Application Deployment data between SA and BSA Essentials.

Platform: All

Subsystem: BSA Essentials Dataminer

Symptom: In SA multimaster environments, it may be observed that deployment data between SA and BSA Essentials does not match. This may occur when the deployment data is replicated across the Model Repository Multimaster Component (vault) to where the BSA Essentials Dataminer is installed within the first few milliseconds of a minute.

Workaround: None.

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 SA 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 the core servers:

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

ISM Tool

QCCR1D: 110511

Description: ISMtool failed to upload ISM into a software policy.

Platform: Windows Server 2008

Subsystem: ISM Tool

Symptom: ISMtool mistakenly identifies a Windows Server 2008 server as a Windows Server 2008 x64 server.

Workaround: If ISMtool detects the registry key HKLM\Software\Wow6432Node on a Windows Server 2008 server, it mistakenly identifies the server as a Windows Server 2008 x64 server. If you are developing an ISM on a server that has this registry key, then temporarily rename the registry during ISM development so that ISMtool will correctly identify the server as a Windows Server 2008 server.

QCCR1D: 111304

Description: ISMTool is not supported on Windows Server 2008 R2 servers.

Platform: Windows Server 2008 R2

Subsystem: ISM Tool

Symptom: Software policies created using ISMTool on Windows 2008 R2 servers cannot be remediated on the same platform.

Workaround: None.

QCCR1D: 111662

Description: ISMControl does not work on Windows 64-bit operating systems for ISMs built using the ZIP package engine.

Platform: Windows Server 2003 x64, Windows Server 2008 x64

Subsystem: ISM Tool

Symptom: The ISMControl command cannot be run on a Windows x64 bit server when a software policy is created using ISMTool with ZIP package in it and remediated on the servers.

Workaround: Replace ZIP packages with MSI packages.

Jobs and Sessions

QCCR1D: 111802

Description: Application Deployment Manager Job Groups sometimes stop refreshing in the SA Client. The refresh rate is also too slow.

Platform: Independent

Subsystem: Jobs and Sessions

Symptom: Currently active Application Deployment Manager jobs will stop updating themselves after a minute or so. This behavior is intermittent.

Workaround: Exit the SA Client and log into the SA Client again.

Model Repository

QCCR1D: 50048

Description: Table owner of PUBLIC SYNONYM AUDIT_ACTIONS changed from TRUTH to SYS.

Platform: All

Subsystem: Model Repository (truth)

Symptom: Previously, SA used PUBLIC SYNONYM on table truth.audit_actions. The PUBLIC SYNONYM on table truth.audit_actions used to get overwritten during Oracle software upgrades.

Also, the use of PUBLIC SYNONYM on truth.audit_actions caused issues with OEM. To fix this issue, the PUBLIC SYNONYM AUDIT_ACTION now points to table SYS.AUDIT_ACTIONS

Workaround: During the upgrade of Model Repository the public synonym is changed. Your Database Administrator can run the following SQL to check the table_owner of this synonym.:

```
> select * from dba_synonyms where synonym_name = 'AUDIT_ACTIONS';
```

OS Provisioning

QCCR1D: 100928

Description: RAID deployment fails for valid RAID configuration on machine with SCSI drives because the “pretty printing” of SCSI drive bus values uses 0-based index instead of 1-based index.

Platform: Red Hat Enterprise Server 5

Subsystem: OS Provisioning

Symptom: RAID deployment fails when the RAID configuration is captured using ACU version 8.35.7.0 (linux5 boot image).

Workarounds: The available workarounds are:

1. Do not deploy RAID policies captured with ACU Version: 8.35.7.0 (linux5 boot image). Instead you should perform captures with ACU Version: 8.25.5.0 (using boot images other than linux5) and deploy those.

2. Modify the raid.hpacu.script custom attribute value for RAID Array Configuration on ACU Version: 8.35.7.0-captured RAID policies to use the correct drive indexes. For example, modify this captured configuration:

```
; Array Specifications
Array= A
; Array Drive Type is Parallel SCSI
; 1:0 (36.4 GB), 1:1 (36.4 GB), 1:2 (36.4 GB), 1:3 (36.4 GB), 1:4 (36.4
GB), 1:5 (36.4 GB)
Drive= 1:0, 1:1, 1:2, 1:3, 1:4, 1:5
```

to the following:

```
; Array Specifications
Array= A
; Array Drive Type is Parallel SCSI
; 2:0 (36.4 GB), 2:1 (36.4 GB), 2:2 (36.4 GB), 2:3 (36.4 GB), 2:4 (36.4
GB), 2:5 (36.4 GB)
Drive= 2:0, 2:1, 2:2, 2:3, 2:4, 2:5
```

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

QCCR1D: 103362

Description: Reprovisioning a server originally provisioned using a Red Hat DHCPless image in an environment with no DHCP server in the VLAN fails.

Platform: Independent

Subsystem: OS Provisioning Backend

Symptom: After a server is provisioned using a RedHat DHCP-LESS image, attempting to reprovision the server causes the server to reboot and after which the reprovision process fails at the Anaconda Configure TCP/IP window, prompting for network information.

Workaround: None.

QCCR1D: 103394

Description: Red Hat DHCPless boot image has no network check warning/error when an IP address that is already in use by another server is specified.

Platform: Red Hat Linux

Subsystem: OS Provisioning Backend

Symptom: When booting a target server using the Linux boot CD in a DHCPless network, specifying an IP address already in use by another host will prevent the target server from successfully registering with the SA core.

Workaround: Make sure the IP address you specify is available.

QCCR1D: 103602

Description: In the Manage Boot Client (MBC) interface, `winpe32-ogfs` and `winpe64-ogfs` image types are not displayed in the PXE image drop-down box.

Platform: Windows

Subsystem: OS Provisioning Backend

Symptom: From MBC's Single Form, after choosing Windows for `OS Family`, the `winpe32-ogfs` and `winpe64-ogfs` PXE types are not displayed. Therefore, you cannot use MBC interface to create `winpexx-ogfs` server records.

Workaround: None.

QCCR1D: 104194

Description: When RAID deployment fails after the RAID controller configuration has been cleared, subsequent RAID captures or deployments will fail unless RAID is first configured manually.

Platform: Independent

Subsystem: OS Provisioning Backend

Symptom: During deployment of a RAID configuration using SA, if the deployment fails after the RAID controller configuration is cleared, subsequent attempts to use SA to capture or deploy RAID configurations to the machine will fail. The following error displays:

```
Exit status: 1280
Error message from ACU: ERROR: (2821) No controllers detected.
```

Workaround: Manually set the RAID configuration. This can be done by booting the machine, pressing F8 when prompted, and then creating logical drive(s) and assigning physical disks and RAID level. After the RAID controller has been manually configured, SA can be used to capture and deploy RAID configurations on the machine.

QCCR1D: 104739

Description: “No driver found” screen displayed during loading of boot image.

Platform: Red Hat Enterprise Server IA64

Subsystem: OS Provisioning

Symptom: During a network boot of a Red Hat Enterprise Linux IA64 server, the following error displays:

```
"No driver found" screen appears:  "Unable to find any devices of the type
needed for this installation type.
Would you like to manually select your driver or use a driver disk?  [Select
driver]  [Use a driver disk]  [Back]"
```

Workaround: The “missing” driver is not required. Press F12 to bypass the driver.

QCCR1D: 109044

Description: OS Build Plan target server is left in `Installing OS` lifecycle if the build plan job times out.

Platform: Windows

Subsystem: OS Provisioning Backend

Symptom: If an OS Build Plan job fails due to a timeout, the target server is left in the `Installing OS` lifecycle instead of the expected `Build Failed` lifecycle state.

Workaround: Reboot the target server into WinPE again. This will reset the lifecycle.

QCCR1D: 110563

Description: Potential issue with writing I18N content to files from OGFS to WinPE.

Platform: Windows

Subsystem: OS Provisioning Backend

Symptom: Data and files containing non-ASCII characters may be corrupted when written to a target server running WinPE under certain circumstances.

Workaround: Use only ASCII characters where possible.

QCCR1D: 111245

Description: `bm.reprovision_attributes_to_preserve` should default to change to new value, rather than keep old value.

Platform: Independent

Subsystem: OS Provisioning

Symptom: If you have customized the `bm.reprovision_attributes_to_preserve` system configuration value, upon upgrade your custom values will be replaced by the new values required for this SA release.

Workaround: Re-enter your values by appending them to this setting on the SAS Web Client **System Configuration ➤ OS Build Manager** page.

QCCR1D: 111337

Description: The `Cannot access target server over OGFS` error occurs randomly on a server while running an OS Build Plan on multiple servers.

Platform: Solaris

Subsystem: OS Provisioning

Symptom: When starting an OS Build Plan job on a Solaris core, the job may fail randomly with a `Cannot access target server over OGFS` error.

Workaround: None.

QCCR1D: 111445

Description: Run OS Sequence does not escalate device group privileges.

Platform: Independent

Subsystem: OS Provisioning

Symptom: Run OS Sequence does not escalate device group privilege. Run an OS Sequence that has an attached device group results in an exception and the job is not created.

Workaround: Enable the Manage Public Device Group privilege for the user group on either the Client Features or Other tab.

QCCR1D: 111781

Description: Specify an alternate drive letter in an OS Sequence when using a WIM image fails.

Platform: Windows Server 2003

Subsystem: OS Provisioning Backend

Symptom: When provisioning Windows Server 2x to a non-`C` drive using a WIM image:

- ¦Windows Server 2003 OS Media works
- ¦Windows Server 2003 WIM fails
- ¦Windows Server 2008 OS Media and WIM fail

Workaround: None.

QCCR1D: 111845

Description: MBC: sequence_id and MAC link was not removed for Solaris10x86 provision done by MBC.

Platform: Red Hat Linux

Subsystem: OS Provisioning - MBC

Symptom: Solaris x86 machines provisioned using MBC may continually reboot into the un-provisioned server pool after initial provisioning.

Workaround: After Solaris x86 provisioning is completed, manually delete the link file (the filename is equal to the target server MAC address) from the core's DHCP server's `/opt/opsware/boot/tftpboot/pxelinux.cfg` directory and then manually remove the sequence_id custom attribute from the server, if it is set.

Patch Management for Solaris

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: Patch Management - Solaris

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: Patch Management - Solaris

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: A workaround is not required because the reboot is performed correctly, even though the display may be incorrect.

QCCR1D: 109142

Description: The default Solaris patch configuration file is overwritten when upgrading to SA 9.0. The Solaris patch configuration file is used by the `solpatch_import` command and is located at `/etc/opt/opsware/solpatch_import/solpatch_import.conf`.

Platform: Solaris

Subsystem: Patch Management - Solaris - Backend

Symptom: If you have modified the default Solaris patch configuration file and you upgrade to SA 9.0, your changes to the configuration file will be overwritten.

Workaround: Save your modified Solaris patch configuration file before performing the upgrade to SA 9.0. After the upgrade, update your Solaris patch configuration file.

Note that Solaris patch bundles are not supported on SA 9.0. For more information, see QCCR1D 109359.

QCCR1D: 109359 and 109361

Description: Solaris patch bundles are supported on SA 7.82 but are not supported on SA 9.0.

Platform: Solaris

Subsystem: Patch Management - Solaris - Backend

Symptom: If you use Solaris patch bundles on SA 7.82 and you upgrade to SA 9.0, SA will give errors when attempting to access the Solaris patch bundles.

Workaround: If you are using Solaris patch bundles on SA 7.82, you can wait for a release following SA 9.0 for support for Solaris patch bundles. Or you can upgrade to SA 9.0 without support for Solaris patch bundles as follows.

1. Remove all Solaris patch bundles from the SA Library. Use either one of the following two methods.

   Method 1 - Remove Solaris bundles using the SA Client.

   a. In the SA Client, select the Library tab and then the By Type tab.
   b. Open the Patches node.
   c. Open the Solaris node.
   d. Locate all the Solaris patch bundles under each Solaris operating system version.
   e. Select each patch bundle and select the Actions ➤ Delete menu.

   Method 2 - Remove Solaris bundles using the `solpatch_import` command.

   a. Put all bundle names in a text file, one bundle name per line. To get a list of existing bundles in the SA Library, run the `solpatch_import` command with the show action and the -q option to display only the bundle names and save the output to a file. The following example command places the bundle names in the file bundles.txt:

   ```
   /opt/opsware/solpatch_import/bin/solpatch_import -a show \
   --all_bundles -q >bundles.txt
   ```

b. Delete the bundles by running the solpatch_import command with the delete action and specifying the text file you created in the previous step. For example:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a delete bundles.txt
```

2. Remove the Solaris patch database by removing the following files, if they are present:

```
/Opsware/Tools/Solaris Patching/solpatchdb.zip
/Opsware/Tools/Solaris Patching/solpatchdb-old.zip
/Opsware/Tools/Solaris Patching/solpatchdb_supplement.zip
```

3. Complete the upgrade to SA 9.0.

4. Create a new Solaris patch database using the following command:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a create_db
```

For complete information on the solpatch_import command and Solaris patching, see the *SA User's Guide: Application Automation*.

QCCR1D: 111342

Description: Because Sun has renamed their Solaris patch clusters, the clusters in your SA Library may not match the cluster names from Sun.

Platform: SunOS 5.6 - 5.10 and SunOS 5.10 x86

Subsystem: Patch Management - Solaris

Symptom: Cluster names in the SA Library do not match cluster names on Sunsolve. Attempting to import clusters with old names using the solpatch_import command will fail.

Workaround: Download the latest supplement file from HP LNc. For complete instructions, see "Obtaining the Solaris Patch Supplementary Data File" in the *SA User Guide: Application Automation*.

Patch Management for Windows

QCCR1D: 102713

Description: The number of rules for patch policy compliance is not correct after remediation or installation of patches.

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: If a patch policy contains one or more superseded patches, the number of total rules counted before remediating the patch policy may be different from the number of total rules after remediating the patch policy. Note that the compliance state of the server is accurate before and after remediating.

Workaround: None.

QCCR1D: 108451

Description: Windows Patch 944036 (installer for IE 8) reports install failure on Windows Server 2008 x64 managed servers.

Platform: Windows Server 2008 x64

Subsystem: Patch Management - Windows - Backend

Symptom: Windows Patching jobs that attempt to install KB944036 (installer for IE 8) will end with an error, and the patch installer returns a non-zero exit code. However, although the patch job reports an install error, the patch is actually installed and subsequent patch and compliance scans will indicate the patch is installed and compliant.

Workaround: A workaround is not required because the patch job succeeded, even though an error displayed.

QCCR1D: 105098

Description: Manually Installing Recommended Microsoft Patch Q934041 (2000) and Q924883 (MS07-014) results in a Non-Compliant server status.

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: Even though the Microsoft patch MS07-024 Q934041 is recommended by Microsoft and is included in the patch supplement, it is not required. If you try to automatically install with a patch policy, it will not install. If you install it manually, it shows a dialog that says: “update has already been applied or is included in an update that has already been applied”. This also applies to patch Q924883 (MS07-014).

Workaround: Since the patch is not required, set a “never install” exception on the patch.

QCCR1D: 110257

Description: Installing March 2010 (or later) MBSA patch database, and specifically patches MS10-015 (KB977165) and MS10-021 (KB979683) on to a Windows Server 2008 x86, the installation does not succeed, even though Patch install Job results indicate success.

Platform: Windows Server 2008 x86

Subsystem: Patch Management - Windows - Backend

Symptom: If you try to install the March 2010 (or later) MBSA patch database, and then attempt to install MS10-015 (KB977165) and MS10-021 (KB979683) on to a Windows Server 2008 x86 using a Windows Patch policy, the Patch install job results will incorrectly indicate success. After a patch compliance scan, SA will still report the patches as recommended for the server, and the server will be listed as non-compliant.

Workaround:

1. To install these patches, import the April 2010 (or later) version of the BSA Essentials Network patch supplement from the BSA Essentials Network on to your SA core server.
2. Visit http://support.microsoft.com/kb/980966/ to download KernelSystemStateCheck.exe to determine whether the patch can be installed on your Windows Server 2008 (x86) managed servers.

3. Contact HP Server Automation Support in order to get this file “qc110257.pyc”. (The Quality Center bug report number is QCCR1D 110257.)
4. On the SA core, copy qc110257.pyc to the SA core’s Data Access Engine (spin) server.
5. As root on the SA Data Access Engine (spin) server, execute the following command:

   ```
   # /opt/opsware/bin/python2 qc110257.pyc
   ```

6. Assuming Microsoft's KernelSystemStateCheck.exe utility reports a pass result, use the ad-hoc Install Patch task window to install the version of MS10-015 (KB977165) that has a file name of Windows6.0-KB977165-x86.msu, and the version of MS10-021 (KB979683) that has a file name of Windows6.0-KB979683-x86.msu.

Note: The Install Patch job progress may show “Was Not Installed” or “side effect” messages. These progress messages may not be accurate. The true indicator of whether these patches installed or not is when after the Install Patch job completes (with reboot), MS10-015 (KB977165) and MS10-021 (KB979683) are no longer recommended, and the compliance indicators for these patches no longer show a red X.

Note: The SA Client will show the mpsyschk.exe version of these patches as recommended or installed.

QCCR1D: 110471

Description: Installer for IE 8 fails to install on a Windows Server 2008 x64 managed server.

Platform: Windows Server 2008 x86

Subsystem: Patch Management - Windows - Backend

Symptom: Attempts to install the patch for KB944036 (Installer for IE8) using SA will fail.

Workaround: Install the patch for KB944036 manually by logging on to the managed server.

SA Client

QCCR1D:105671

Description: The SA Client cannot be installed under a localized (I18N) directory.

Platform: Windows

Subsystem: SA Client Framework

Symptom: Cannot install the SA Client Launcher in a path containing non-ascii characters.

Workaround: Install the SA Client Launcher in a path containing only ascii characters.

SA/NA Integration

QCCR1D:90653

Description: A workaround is needed to integrate SA 7.8x and SA 9.x with NA7.5x.

Platform: Independent

Subsystem: SA/NA Integration

Symptom: SA/NA Integration fails.

Workaround: In the `jboss_wrapper.conf` file, comment out the following lines:

```
#wrapper.java.additional.6=-Dorg.omg.CORBA.ORBClass=com.sun.corba.se.internal
.Interceptors.PIORB
#wrapper.java.additional.7=-Dorg.omg.CORBA.ORBSingletonClass=com.sun.corba.se
.internal.corba.ORBSingleton
#wrapper.java.additional.8=-Xbootclasspath/p:/opt/NA/server/ext/wrapper/lib/
CORBA_1.4.2_13.jar
```

After you have commented out these lines, restart `truecontrol`.

SA/OO Integration

QCCR1D:102614

Description: Before integrating SA with any HP Operations Orchestration (OO) flows using the SA Client, you must import the OO SDK Client certificate. Make sure that the version of the OO SDK Client Certificate is compatible with the version of OO you plan to use with SA. Typically, you can import the certificate once and the same OO SDK Client Certificate will support different versions of OO. SA 9.0 contains an OO SDK Client Certificate for OO version 7.51, which also supports OO versions 7.6 and 9.0. See the *SA Integration Guide* for information on how to import the OO SDK Client Certificate.

Platform: Independent

Subsystem: SA/OO Integration

Symptom: The SA/OO Integration feature is not available until after you import the required OO SDK Client Certificate.

Workaround: If you have a mesh core containing one master core and one or more slave cores, complete the following steps for the Web Services Data Access Engine (twist) component on the master core and on all slave cores.

If you have a sliced core installation containing one or more slices, complete the following steps for the Web Services Data Access Engine (twist) for each slice.

1. Enter the following command to stop the twist component:

   ```
   /etc/init.d/opsware-sas stop twist
   ```

2. Enter the following command to export the OO Central Certificate:

   ```
   /opt/opsware/jdk1.6/jre/bin/keytool -exportcert -alias pascert -file /tmp/
   oocentral.crt -keystore /var/opt/opsware/twist/oocert
   ```

3 Import the OO Central Certificate to the SA JRE Keystore. The JRE keystore default password is `changeit`.

```
/opt/opsware/jdk1.6/jre/bin/keytool -importcert -alias pas -file /tmp/
oocentral.crt -keystore /opt/opsware/jdk1.6/jre/lib/security/cacerts
```

4 Make sure there are no errors when you entered the previous commands.

5 Enter the following command to make sure the certificate was imported successfully:

```
/opt/opsware/jdk1.6/jre/bin/keytool -list -alias pas -keystore /opt/
opsware/jdk1.6/jre/lib/security/cacerts
```

Example output:

```
pas, Feb 3, 2010, trustedCertEntry,
Certificate fingerprint (MD5):
DF:DD:22:1B:A2:1E:A9:9C:1C:AF:8F:E0:14:1F:B5:E0
```

6 Enter the following command to start the twist:

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

QCCR1D: 111738

Description: When a Run Flow job for SA/OO Integration fails due to a timeout in SA, the “Open report in HP Operations Orchestration” menu action displays as selectable, gray text. When you select this action, a “Cannot redirect to Operation Orchestration” error message displays.

Platform: Independent

Subsystem: SA/OO Integration

Symptom: The Run Flow job in Operations Orchestration (OO) took longer than the timeout value configured in SA. In OO, the flow run could have run successfully or failed. In SA, the job fails, based on the timeout value configured in SA. If you click the hyperlink for click-n-launch (“Open report in HP Operations Orchestration”), you will not be able to see details about whether flow run was successful or failed in HP Operations Orchestration (OO). It is important to see the details—if the flow just took longer, then you can fine tune the timeout value in SA.

Workaround: Author flows in HP Operations Orchestration (OO) using `saJobId` as flow input, for the flows to be run using SA and then search for flows in HP Operations Orchestration (OO) using `saJobId` as the input name and the value of `JobId` from SA as the value. Alternatively, log on to Operations Orchestration in a browser and look for the flow run and match it to a Run Flow job in SA.

SA/SAR Reports

QCCR1D: 105234

Description: Connections by Network Device not yielding results when equals operator is used.

Platform: Independent

Subsystem: SA Client Reporting

Symptom: In the SA Client in an NA-enabeld core, if you run the Connections by Network Device report and set the parameter to Device Name Equals [Any Value], the search returns no results.

Workaround: Run the report using the following parameters:

> Device Contains <leave blank to return all network devices and their physical connections or specify the name of a network device>

QCCR1D: 107293

Description: Scheduled reports exported to .xls do not display charts or graphs.

Platform: Independent

Subsystem: SA Client Reporting

Symptom: If you schedule a report, select the .xls format. The attachment is received with an “Unsupported Image error” in place of the chart or graph. However, tables are sent correctly. Graphs are not visible in the .xls file, but the report should not display empty image blocks.

Workaround: None.

QCCR1D: 112434

Description: Folder definitions are missing in the `report_def.xml` file, in the BSA Essentials 2.0/2.01 installation patch. These definitions are required to view the Application Deployment and Windows patch reports in the BSA Essentials/SAR Client.

Platform: Independent

Subsystem: SA Client Reporting

Symptom: You do not see the “Application Deployment” and “Patch” folders and their reports in the BSA Essentials/SAR Client.

Workaround: After you complete the installation process the for BSA Essentials 2.0/2.01 patch and download content from the BSA Essentials Network for the product/stream you subscribe to, complete the following steps:

1. Log in to a BSA Essentials core server.
2. Chnage your user to become the BSA Essentials super user on the server:

   ```
   su - omdb
   ```

3. Enter the following commands:

   ```
   cd /opt/opsware/omdb/deploy/birt.war
   cp report_def.xml report_def_org.xml
   vi report_def.xml
   ```

4. Add the following two lines in the `<folders>` section of the `report_def.xml` file:

   ```
   <subfolder_name>application_deployment_reports</subfolder_name>
   <subfolder_name>top_level_patch_reports</subfolder_name>
   ```

   Example:

   ```
   <folder name="reports">
   <display_name>Reports</display_name>
   ```

```
<folder_reports></folder_reports>
<subfolders>
<subfolder_name>application_deployment_reports</subfolder_name>
<subfolder_name>top_level_patch_reports</subfolder_name>
.....
.....
</subfolders>
<parent>none</parent>
</folder>
```

5 Save the `report_def.xml` file.

6 Launch the BSA Essentials Java Client.

7 Click on the Reports folder to see the “Application Deployment” folder and “Patch” folders.

SAS Web Client

QCCR1D: 109000

Description: Internet Explorer Enhanced Security Disables some SAS Web Client features

Platform: Any

Subsystem: SAS Web Client

Symptom: If you are using Internet Explorer Enhanced with Security Configuration (IE ESC) enabled to access the SAS Web Client, this configuration blocks some features of SAS Web, such as the search function.

Workaround: There are two solutions to this issue:

1. Add the SAS Web core URL to IE's trusted sites list.

When using IE with ESC enabled to access the SAS Web Client core login page, you will be asked whether or not to trust the core web site. You must click the Add button in order to add the core web site to the list of trusted sites.

To Manually add the core URL to the trusted sites list, in IE select Tools ➤ Security ➤ Trusted Sites. Enter the entire URL (for example, https://192.168.181.130) and then click **Add**. Restart your browser to ensure all new settings are accepted.

2. Disable IE ESC altogether.

Go to the Server Manager (the first icon near the Start Menu on most systems, or the top left hand side icon on all configurations). The Server Manager view should be automatically selected on the left side panel. On the right side panel, there is a Group label named Security Information. On the right hand side of the pane, in Security Information, click the link named Configure IE ESC. For both Administrator and Users, select Off and then click **OK**. Restart your browser. IE ESC is now disabled.

QCCR1D: 111394

Description: A cloned user group is missing some OGFS privileges.

Platform: Independent

Subsystem: SAS Web Client

Symptom: Privileges for only one login is copied to the cloned user group. If the existing user group has OGFS privileges for multiple users/logins, privileges are copied only to one cloned user group.

Workaround: Go to **OCC** ➤ Groups and the newly cloned group. Select the OGFS tab and add other missing logins for OGFS privileges.

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.

Script Execution

QCCR1D: 79545

Description: Exporting a Run Server Script Job with or containing multi-byte characters (Japanese/Korean) to .csv results in question marks.

Platform: Windows

Subsystem: Script Execution

Symptom: If you export a Run Server Script job output that has multi-bytes characters (Japanese / Korean) to a CSV file, the file contains question mark (???) characters.

Workaround: Export the job results in .txt format to eliminate the garbled text.

SE Connector

QCCR1D: 105778

Description: After deploying the SE Storage Scanner on hosts, select **Administration ➤ Storage Scanners**. In the list of names for the SE Storage Scanner on "Host", the host name is missing on some of them.

Platform: VMware

Subsystem: SE Connector

Symptom: When a server on which SE Connector is running is directly deactivated and deleted, stale entries of Storage Scanners will be visible in the Storage Scanner browser. The stale entries count will be increased, depending on how many times the server is deactivated and deleted from a core.

Workaround: Manually delete the stale entries from the Storage Scanners browser, whose server reference objects are null.

Server Automation Installer

QCCR1D: 111215

Description: Restoring OS Provisioning Stage 2 images fails on SUSE Enterprise Linux 9.

Platform: SUSE Enterprise Linux 9

Subsystem: Installer

Symptom: Restoring Stage 2 images fails on SUSE Enterprise Linux 9, which is a deprecated platform.

Workaround: You can restore the OS Provisioning Stage 2 images by manually running the restore_stage2.pyc script. This script is located in:

```
<distro>/opsware_installer/tools/restore_stage2.pyc
```

Software Management

QCCRID: 100754

Description: You cannot set the timeout 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 timeout 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 timeout value to greater than 5 hours, the job still times out after 5 hours. If you set the timeout value to less than 5 hours, the timeout 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 timeout 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: 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`.

QCCR1D: 102934

Description: Web Services Data Access Engine (`twist`) cache full exception encountered while running compliance across 500 servers.

Platform: Independent

Subsystem: Software Management - API - Compliance

Symptom: You encounter problems when running a large remediate job.

Workaround: Increase the cache size.

QCCR1D: 111356

Description: Problem with Webservice invocation on UAPI `SoftwarePolicyService.Create()`.

Platform: Independent

Subsystem: Software Management - API - Software Policy

Symptom: When using WebService API invoke `SoftwarePolicyService.create()`, if you set the RPM package in the installable item list by using `setInstallableItemData()`, the install list is not created.

Workaround: Use UAPI or `webServiceAPI` by calling `setSoftwarePolicyItems()`.

Storage Host Agent Extension

QCCR1D: 107944

Description: Storage Visibility and Automation is not supported on ESX 3.0.x.

Platform: VMware ESX 3.0.x

Subsystem: Storage Host Agent Extension

Symptom: Running a storage snapshot specification on an ESX 3.0.x servers results in an error message that indicates unsupported namespace in content of SOAP body. As a result, storage related information for ESX 3.0.x is not stored and displayed in the SA Client.

Workaround: None.

Virtualization

QCCR1D: 90019

Description: A unique constraint violation occurs when scanning servers that have duplicate virtual network names.

Platform: Windows Server 2008/Hyper-V

Subsystem: Virtualization

Symptom: If a system has more than one virtual network with the same name, even if they are managed by different hypervisors, scanning for virtual servers fails due to a violation of unique name constraints.

Workaround: Do not use duplicate virtual network names.

QCCR1D: 106085

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 Server 2008 pre-R2 server

Subsystem: Virtualization - Hyper-V

Symptom: SA may change the Management IP address from the one you registered to one of the other IP addresses. This only occurs on Windows Server 2008 pre-R2 servers.

Workaround: To prevent this problem, you need to manage your Windows 2008 pre-R2 server from a Windows 2008 R2 server and make sure the option to allow the management operating system to share the network adapter is not selected. The following gives the basic steps to accomplish this, however, see your Microsoft Hyper-V documentation for complete details. More information may also be available by searching the internet for “New in Hyper-V Windows Server 2008 R2” and “Hyper-V Remote Management: You do not have the required permission to complete this task.”

1. Make sure the administrators on the pre-R2 and R2 servers have the same password.
2. Log on to the R2 server and start the Hyper-V Manager applet.
3. Right-click on the Hyper-V Manager and select Connect to Server.
4. In the Select Computer window, select the “Another Computer” radio button and enter the name of the pre-R2 server.

   An icon for the pre-R2 server will appear in Hyper-V Manager.
5. Select the icon for the pre-R2 server and open the Virtual Network Manager.
6. Highlight the NIC whose configuration you need to change.
7. Under the Connection type, unselect “Allow management operating system to share this network adapter.”
8. Click **OK**.

QCCR1D: 104418

Description: The reported OS property for ESX servers is inconsistent between direct (SA Agent) and indirect managed (vCenter) cases.

Platform: VMware ESX (all versions)

Subsystem: Virtualization - Backend (VMWare)

Symptom: OS property text is different from what is reported by the Agent and what is reported by VS.

Workaround: None.

QCCR1D: 105999

Description: There are cloning problems with agent revival if initial registration failed.

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

Symptom: After cloning an SA managed virtual machine, when the clone starts up for the first time and in case there is no network connectivity on the clone, agent revival will fail to create a new server record for the cloned MVM.

Workaround: Restart the agent on the cloned machine after network issues are resolved and the agent will correctly register as a cloned MVM.

QCCR1D: 106909

Description: Windows Shutdown Event Tracker must be disabled on the source Windows Virtual Server for a Clone Virtual Machine job to complete registration of the SA server. Windows 2003 x64 cloning requires a manual reset to resume virtual machine images customization.

Platform: Windows

Subsystem: Virtualization

Symptom: Clone Virtual Machine job will fail the Registering Server step if the Windows Shutdown Event Tracker is enabled on the source virtual machine. This is because the Shutdown Event Tracker waits for user input before it completes rebooting, so the SA Agent registration cannot complete.

Workaround: Disable the Shutdown Event Tracker on the clone source virtual server.

QCCR1D: 109849

Description: Add vCenter, whose hypervisors are already managed by SA, fails with “integrity constraint (TRUTH.DEVICES_VSWITCH_INTERFACES_FK) violated - parent key not found”.

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

Symptom: On vCenter Reload, an error message indicates that the reload failed.

Workaround: Try Reload again.

QCCR1D: 109887

Description: The snapshot view is not available on an ESX server that is managed by vCenter.

Platform: Red Hat Linux

Subsystem: Virtualization

Symptom: Snapshot view is not available for ESX managed servers

Workaround: Manage ESX directly snapshot view.

QCCR1D: 110035

Description: After removing the VS of a dual-managed ESXi server, hypervisor credentials do not display in the Properties view.

Platform: VMWare ESXi

Subsystem: Virtualization

Symptom: When a hypervisor that is dual-managed (through Virtualization Service and SA Agent) loses one of its management paths (such as when. the Virtualization Manager or VCenter is removed from SA), the Login Credentials panel does not display in the server browser panel.

Workaround: Right-click on the hypervisor, select “Refresh Server”, and then press F5 (Refresh) to refresh the client so that the Login Credentials panel displays in the server browser.

QCCR1D: 111307

Description: The “add ESXi” operation suspends processing.

Platform: ESXi

Subsystem: Virtualization - Backend (VMWare)

Symptom: Adding an ESXi server with larger hardware configuration data will suspend processing.

Workaround: Reconfigure the server with fewer cpu counts in hardware information.

QCCR1D: 111363

Description: Modify Virtual Machine fails when trying to modify or remove vlan adapter types VMXNET 2 or VMXNET 3.

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

Symptom: Virtual Machine job fails if you try to change the network connection or remove a virtual network adapter of type VMXNET2 or VMXNET3.

Workaround: Use VMware vCenter to modify this virtual network type.

QCCR1D: 111789

Description: Adding two vCenters concurrently results in one of the automatically triggered reload data to suspend processing.

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

Symptom: Two concurrent vCenter additions will take a long time and might suspend processing.

Workaround: Add the vCenters separately.

QCCR1D: 111922

Description: Create Virtual Machine on an SA managed ESX 3.5 server fails with an error message of `com.vmware.vim25.VirtualMachineConfigSpec`.

Platform: ESX 3.5

Subsystem: Virtualization - Backend (VMWare)

Symptom: The Create Virtual Machine operation fails.

Workaround: After the SA 7.5 release, one of the VMM library jar files was changed from `OPSWvmm-vmware.jar` to `vmm-vmware.jar`. When an upgrade is performed from SA 7.5 directly to SA 9.0, or from SA 7.5 to SA 7.8 to SA 9.0, and any virtualization operation is invoked on the ESX hypervisors, the VMM package gets remediated first with the new package but the `OPSWvmm-vmware.jar` file is left untouched. This causes the consecutive virtual machine create operations to fail.

The following workaround is intended for any ESX hypervisor that is managed by an Agent in SA and whose virtualization aspect will still be handled through the same route (not via VS) in SA 9.0.

1. Create a script.
   a. From the Navigation pane, select **Library ➤ By Type ➤ Scripts ➤ Unix**.
   b. From the Actions menu, select **New** and then enter the following information:

      Name: Clean VMM on ESX

      Location: Select **Package Repository ➤ All VMWare Linux ➤ VMWARE ESX Server** <any version>

      Script Content:

      ```
      1. unlink /opt/opsware/vmm/lib/OPSWvmm-vmware.jar > /dev/null 2>&1
      ```
   c. **Description**: Enter a brief description, as necessary.
   d. Leave the defaults for the remaining fields and then select **File ➤ Save** to save and close the window.
2. Create a dynamic device group and add the target servers to this device group.
3. Run the script on the servers in the device group created above.

➤ This script can be used on all ESX versions. There is no need to duplicate it in different packages or to create a separate device group for each hypervisor version.

QCCR1D: 111972

Description: Create Virtual Machine fails on a directly managed ESX hypervisor if the virtual machine’s datastore name contains special characters.

Platform: ESX

Subsystem: Virtualization - Backend (VMWare)

Symptom: The Create Virtual Machine job fails when the datastore name contains special characters.

Workaround: Change the datastore name so that it does not contain special characters.

Web Services Data Access Engine

QCCR1D: 111039

Description: Out-of-memory error.

Platform: Red Hat Linux/Solaris

Subsystem: Web Services Data Access Engine (`twist`)

Symptom: An out-of-memory error is encountered in the Web Services Data Access Engine

Workaround: The default maximum heap size for Web Services Data Access Engine has been increased to 2560MB from 1280MB.

QCCR1D: 112222

Description: The default maximum JVM heap size has been increased to 2560 MB, and as a result, the Web Services Data Access Engine (`twist`) does not start properly on Linux AS3 32-bit systems due to a two gigabyte memory limit for a single process running on JVM on 32-bit systems.

Platform: Red Hat Enterprise Linux AS3 32-bit

Subsystem: Web Services Data Access Engine (`twist`)

Symptom: The Web Services Data Access Engine (`twist`) does not start and records the error: `Could not reserve enough space for object heap` in:

```
/var/log/opsware/twist/boot.log
```

Workaround: Before upgrading, edit the file:

```
/etc/opt/opsware/twist/twistOverrides.conf
```

and add the following entry:

```
twist.mxMem=<memory size in Megabytes>
```

The value must be 2000 megabytes or less.

For example:

```
twist.mxMem=1960m
```

5 Documentation Errata

This chapter contains information that corrects or updates the SA online Help and product manuals.

To check for updates, 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, select the **New users - please registe**r link on the HP Passport login page.

Updated Quick Start Videos Available

You can download the latest version of *Quick Start with Server Automation* videos that quickly show you how to use HP Server Automation by going to the HP Software Product Manuals web site. For instructions, see Download the Latest Quick Start Videos on page 12.

Application Deployment Manager

The following section provides additional information about documentation for the Application Deployment Manager feature.

Context-Sensitive (F1) Help

In the Application Deployment Manager, context-sensitive online help is provided for numerous dialogs, including the Manage Applications and Manage Targets dialogs.

To view a context-sensitive help topic, click the question mark icon ? in the dialog. Note that the F1 key does not open online help for the Application Deployment Manager.

To view the portion of the SA online help that pertains to application deployment, select Help ➤ Help in the Application Deployment Manager.

Refer to the *HP Server Automation Application Deployment Manager User Guide* for additional information.

SA/OO Integration

The following sections provide additional information about documentation for the SA/OO Integration feature.

SA Integration Guide

See the *SA Integration Guide* for information about this new feature. This document is available on the HP Product Software Manuals site, through the HP Passport portal at http://h20230.www2.hp.com/selfsolve/manuals.

Context-sensitive (F1) Help

F1 Help is not available in this release. See the *SA Integration Guide* for information about this new feature.