HP Server Automation

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

Software Version: 7.80

Release Notes

Document Release Date: December 2009
Software Release Date: June 2009

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

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

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

http://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
	June 2009	Document Created
3 Known Problems, Restrictions, and Workarounds in SA 7.80	September 2009	Added defects 93876 and 93840.
3 Known Problems, Restrictions, and Workarounds in SA 7.80	December 2009	Added known issues QC 93782/96506, QC 102450, QC 102318, QC 102965

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 7.80

HP Server Automation (SA) 7.80 automates critical areas of server and application operations — including the provisioning, patching, server and application configuration change management, compliance checking and reporting — across major operating systems and a wide range of software infrastructure and applications.

The following sections describe all new features and enhancements in the SA 7.80 release.

For information regarding new features for the HP Storage Visibility and Automation and the HP Service Automation Reporter (SAR) clients, please refer to the *Release Notes* for those products.

Storage in SA — Disclaimer

SAN storage capabilities will not be available in SA until SE 6.1.1 is released. Until the SE 6.1.1 is released, SA documentation will document storage capabilities that are not available.

Increased Slice Component Bundle Memory Requirement

The recommended memory requirement for servers hosting a Slice Component bundle is now increased to 8GB from 4GB.

SA Bus Replaces TIBCO

As of SA 7.80, TIBCO Rendezvous has been replaced by the SA Bus. The SA Bus is a set of libraries that provide a certified messaging services. The SA Bus replaces TIBCO automatically during upgrade, no additional user configuration is required.

SA 7.80 Ships with Oracle 11g

The version of the HP-supplied Oracle database is *Oracle Database Standard Edition 11g*. Oracle 10g is still supported for existing or manually installed databases. For manual installations, SA supports both the Oracle Database Standard Edition and the Oracle Database Enterprise Edition.

Software Repository Moves to Slice Component Bundle

As of SA 7.80, the Software Repository has moved from the Infrastructure Component bundle to the Slice Component bundle. Because you can install multiple instances of the Slice Component bundle, there can now be *multiple instances of the Software Repository.*

A component called the *Software Repository Store* remains as part of the Infrastructure Component bundle and handles NFS exports to Slice Component bundle hosts. The Software Repository Store can be installed on any server hosting an Infrastructure Component bundle. You can also choose not to install the Software Repository Store, but you must manually configure an NAS (filer) to allow Slice Component bundle servers access to the file system.

Satellite Compatibility

When you upgrade a Core to SA 7.80, certain directories are retained for Satellite backward compatibility for ESX/Linux OS Provisioning. These directories are prefixed with `bi-` and are found in:

`/opt/opsware/buildscripts/linux`

on the server hosting the Build Manager (`buildmgr`).

However if you add a new Slice Component bundle *during* the Core upgrade, these `bi-` directories are not created. Therefore, a new Slice Component bundle added during an upgrade does not support Satellite backward compatibility for ESX Server / Linux provisioning.

If you must maintain support for ESX/Linux OS Provisioning but must also support pre-SA 7.80 Satellites, you must manually copy the `bi-` directories from the old Slice Component bundle host to the new host.

Alternatively, you can Upgrade the Satellite to SA 7.80 before adding any new Slice Component bundles.

The following is a list of the `bi-` directories:

`bi-2.1AS`

`bi-2.1ES`

`bi-2.1WS`

`bi-3AS`

`bi-3AS-IA64`

`bi-3AS-X86_64`

`bi-3ES`

`bi-3ES-IA64`

`bi-3ES-X86_64`

`bi-3WS`

`bi-3WS-IA64`

`bi-3WS-X86_64`

`bi-4AS`

```
bi-4AS-X86_64
bi-4ES
bi-4ES-X86_64
bi-4WS
bi-4WS-X86_64
bi-5CLIENT
bi-5CLIENT-X86_64
bi-5SERVER
bi-5SERVER-X86_64
bi-ESX-3
bi-SLES-10
bi-SLES-10-X86_64
bi-SLES-8
bi-SLES-9
bi-SLES-9-X86_64
bi-SUSE-8.0
bi-bootagent
```

Solaris Patch Management Improvements

HP Server Automation 7.80 adds to its support for Solaris patches, patch clusters and Solaris patch policies. SA 7.80 automates the process of keeping your Sun Solaris servers running with current patches. With SA you can:

- Download Solaris patches and store them in the SA library.
- Create Solaris patch policies from downloaded Solaris patches.
- Download information associated with each patch including:
  - Platform settings including support for multiplatform patches
  - Patch dependencies
  - Reboot settings
  - Vendor documentation
- Install patches by remediating Solaris patch policies. Remediation automatically handles various patch reboot settings including single-user mode, reconfiguration reboot and reboot immediate.
- Perform compliance scans including server platform and patch supersedence applicability checks.
- Patch Solaris zones.

For more information, see “Solaris Patching” in the *SA User’s Guide: Application Automation*.

Previous to SA version 7.8, SA stored separate copies of each patch for each version of the OS the patch applied to. For example, if a particular patch applied to Solaris 8, 9 and 10, SA would store three separate copies of the patch.

As of SA 7.8, SA stores only one copy of each patch along with the list of OS versions the patch applies to. If you upload a new version of a patch that already has multiple copies stored in SA, SAwill replace the multiple older copies with one copy of the updated patch and store the list of OS versions the patch applies to.

Windows Patch Management Improvements

In SA 7.80, if Windows permits a patch to be uninstalled, you can uninstall Windows Service Packs and Update Rollups using SA. The installed Server Agent must be an SA 7.80 Agent and the service pack or update rollup must have been installed using SA.

Managed Server (Agent) Platform Support

As of SA 7.80, the infrastructure for adding support to SA for additional Managed Server platforms is in place. However, the first available additional platforms will be made available in a later SA 7.80 patch release.

Red Hat Linux 4 Update 7

Red Hat 4 Update 7 is vulnerable to kernel panics, to avoid them you must update your kernel (see *https://bugzilla.redhat.com/show_bug.cgi?id=456993*). You can get the updated kernel here:

http://people.redhat.com/vgoyal/rhel4/RPMS.kernel/

Locales and Agent Version

All SA Server Agents using locales other than English, Japanese or Korean must be upgraded to SA 7.80. Agents of earlier versions are not supported with locales other than English, Japanese and Korean.

Service Automation Visualizer

Service Automation Visualizer (SAV) 7.80 is released as part of the SA 7.80 release and provides the following new features:

- VMware ESXi Server 3.5: Support for virtualization relationships between hypervisors and their VMs, including physical and logical relationships between hypervisors and VMs, as well as relationships to other servers.
- Storage visibility support for VMware ESX and ESXi hypervisors and their virtual machines, such as HBAs and ports, file systems, and dependencies on remote storage and switches and arrays.
- Support for Storage Visibility and Automation: SAV 7.80 allows you to view storage and SAN information as well as the logical and physical storage connections between SAN devices with an SA core that is configured to connect to Storage Essentials (SE). For more information, see the Storage Visibility and Automation documentation.
- Support for Microsoft Windows Server 2008 Hyper-V virtualization technology: Full support for visualizing Microsoft's virtualization technology, displaying virtualization relationships between hypervisors and their VMs, including process information, physical a logical relationships between hypervisors and VMs, as well as relationships to other servers, network devices, storage devices, and so on.

Secure Data Storage API

SA 7.80 adds Secure Custom Attributes (SCA) and Secure Virtual Columns (SVC) to enable applications to store sensitive data in a secure manner. This is provided through the SA API in the CustAttrNamespaceService interface. Any SA applications that need to securely store sensitive data, such as user credentials, can use this interface. Access to data in SCAs and SVCs is enforced by the SA security framework.

For more information, see the CustAttrNamespaceService interface in the com.opsware.custattr package in the SA API documentation and the *SA Platform Developer's Guide*.

VMware ESXi Support

In this release, SA adds support for the VMware ESXi 3 server. The VMware ESXi server is functionally equivalent to the ESX 3 servers, however, in the ESXi, the Linux-based service console (COS) has been removed. As a result, SA does not install an Agent on ESXi servers. Instead, SA manages ESXi servers remotely using a web services interface. ESXi servers are listed in both the All Managed Servers and Virtual Servers lists of the SA Client the same as other ESX servers. However, some SA features are not available for ESXi servers.

For more information, see "Virtual Server Management" in the *SA User's Guide: Server Automation*.

Storage Visibility and Automation & SE Integration

In this release, Storage Visibility and Automation is a feature in SA 7.80 that enables storage supply chain information in the SA product line—SA, SAV, and SAR. While Storage Visibility and Automation is included as part of the Server Automation (SA) 7.80 release, it also requires Storage Essentials (SE) 6.1.1 for storage data discovery.

Storage Visibility and Automation collects storage information from Storage Essentials (SE) discovery and enables storage information in SA, as follows:

- Host server storage information is discovered by the Storage Host Agent Extension in Storage Visibility and Automation—and not by SE discovery.
- Database storage information is discovered by a Storage Scanner in Storage Visibility and Automation—and not by SE discovery.

SE discovers information about the SAN arrays, switches, fabrics, and NetApp filers in your environment. SA obtains information about these storage assets from SE. Storage assets that are enabled in SA include SAN arrays, fabrics, controllers, and zones. Storage Visibility and Automation also provides information about connectivity, such as the relationship of a switch and a managed server.

This feature replaces its legacy product, known as Application Storage and Automation System (ASAS).

Device Group and Search Enhancements - Search on a Subnet

You can now perform searches and create device groups that contain servers on a particular subnet. You can use an IP address and either a subnet mask or a CIDR number to specify the network address of the subnet.

For more information, see “Device Groups” and “SA Client Search” in the *SA User’s Guide: Server Automation*.

Internet Information Services (IIS) 7 Support

In this release, the Windows IIS 7.0 server module allows you to view various elements and configuration of a server’s IIS 7.0 application, such as Application Pools, Web Sites, and Features.

You can add the Windows IIS 7.0 server module to a Software Policy, attach it to other servers, and then remediate (install) onto other servers running IIS 7.0 and force them to conform to your company’s standards.

If you select Add to Library, the IIS 7.0 configuration item becomes accessible to other users on your data center, for use specifically in software policies.

You can also use the Windows IIS 7.0 server module inside of audits and snapshot specifications. In a snapshot specification, you can capture the state of your IIS configuration on a server you know to have a good configuration (a “golden” server), and use that to compare against other target servers running IIS 7.0. You can also use Audits to check a server’s IIS 7.0 configuration on a time or regular basis, so you can keep track of a server’s IIS 7.0 configuration, and remediate the server if it ever becomes “non-compliant.”

Audit and Remediation Enhancements

In this release, the Audit and Remediation feature has been enhanced to include the following new features:

- Audit policies have been enhanced to provide linking to multiple audit policies within a policy. For example, you could combine several different discrete audit policies together one master policy that defines how Windows services should be configured. After you run the audit, if any discrepancies are discovered you can remediate them from the audit results.
- The new Compliance Check Editor allows you more easily manage your BSA Essentials Subscription Services compliance checks for audits and snapshots. With the Compliance Check Editor you can browse, regroup, and edit property information (metadata) about your core's compliance checks.
- A new compliance rule, the Microsoft Internet Information Server, enables you to use real time information about IIS for your audit, such as a Windows server, such as server name, server type, server state, log file path, document file path, and so on.
- Audits now have a “re-run” feature that allows you to more easily rerun an audit at your convenience.
- For the Windows Registry rule you can now configure file and directory inclusion and exclusion rule parameters.

Support for Microsoft Hyper-V/Virtual Machine Manager (VMM)

SA 7.80 virtual server management supports the following *Microsoft Hyper-V virtual machine* tasks:

- Shutdown
- Power Off
- Pause
- Reset (reboot)

For more information, see “Virtual Server Management” in the *SA User’s Guide: Server Automation*.

Automation Platform Extension Enhancements

SA 7.80 adds a new way of running Automation Platform Extensions (APX). You can run extensions from Managed Servers, by selecting a server first. You can select one or more servers in the SA Client, then right click or select the Actions menu and select the Run Extension menu item. This applies only to certain program extensions.

For more information, see “Running SA Extensions” in the *SA User’s Guide: Application Automation*.

Extensible Discovery

SA 7.80 adds Extensible Discovery, a way to gather custom information from your managed servers. SA can gather a large amount of information from your servers by default. Extensible Discovery lets you gather additional information about your servers quickly and easily. Extensible Discovery is a feature that you can customize and use to discover and obtain custom information about servers in your managed environment.

For more information, see "Running SA Extensions" and Running Extensible Discovery on Managed Servers" in the *SA User's Guide: Application Automation*.

Core Recertification Enhancements

SA 7.80 provides a *Core Recertification Tool* that allows you to recertify SA Cores and Agents. The Core Recertification Tool automates and speeds up the process of issuing new security certificates as compared to previous releases. This tool is separate from and compatible with the existing Agent recertification tool, also known as Server Recert Custom Extension utility.

Major advantages of the Core Recertification Tool are:

- The ability to regenerate all SA certificates before their expiration, which effectively shorten their life span
- The ability to mitigate certificate compromises.

SA/Operations Orchestration Integration

Operations Orchestration (OO) will not integrate with SA 7.80 until a patch for OO is released and applied in the near future. Contact SA Technical Support if you must integrate OO with SA 7.80.

Deprecated Features in SA 7.80

The following features are being deprecated in this release:

Code Deployment and Rollback (CDR) and Configuration Tracking

Code Deployment and Rollback (CDR) is deprecated but still supported in SA 7.80. It will not be supported as of SA 8.0. For more information, contact your HP sales representative.

DOS-Based OS Provisioning

DOS-based OS Provisioning is being deprecated in this release and will no longer be available as of SA 8.0. For more information, talk to your HP sales representative.

No Longer Available in SA 7.80

start_opsware.sh and stop_opsware.sh Scripts

Previous versions of SA provided two scripts, `start_opsware.sh` and `stop_opsware.sh`. As of
SA 7.80, these scripts are no longer supported. You must use the unified start script, `/etc/init.d/opsware-sas`. If you have any applications or scripts that depend on these two scripts, you must rewrite them to use the unified start script.

Documentation for Server Automation 7.80

This release comes with the following documentation:

- *SA Release Notes*
- *SA Quick Reference: Pre-Installation Requirements*
- *SA Planning and Installation Guide*
- *SA Upgrade Guide*
- *SA Policy Setter's Guide*
- *SA Administration Guide*
- *SA User's Guide: Server Automation*
- *SA User's Guide: Application Automation*
- *SA Oracle Setup for the Model Repository*
- *SA Content Utilities Guide*
- *SA Content Migration Guide*
- *SA Platform Developer's Guide*

2 Platform and Environment Support for SA 7.80

Supported Operating Systems for SA 7.80

See the document *SA 7.80 Supported Platforms* 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 Known Problems, Restrictions, and Workarounds in SA 7.80

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

Bug ID: 155270 / QCCR1D: 66624 (See also 154714/66068)

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

Platform: Independent

Subsystem: Agent Installer

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

```
[INFO] Stopping Opsware agent.
[INFO] Removing non-legacy agent files.
[INFO] Installing Opsware agent into 'C:\Program Files\Opsware\agent'.
[INFO] Agent unpack deferred to InstallN() for atomic delivery.
[ERROR] Opsware agent installation failed.
[ERROR] Unable to open service : 'opswareagent' : Error : (1060) : 'The
specified service does not exist as an installed service.'.
[ERROR] Opsware agent could not be started.
[WARN] Unable to remove directory
'C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~1804-1.WRK' : Error : (32) : 'The
process cannot access the file because it is being used by another process.
```

Workaround: Uninstall the SA 6.5.1.2 agent then install the SA 6.5.1.3 agent.

QCCR1D: 92318

Description: Agent installer does not launch when provisioning a Windows Server 2003 x86 (Japanese R2SP2) using Windows PXE boot.

Platform: Windows

Subsystem: Agent Installer

Symptom: While provisioning a Windows Server 2003 x86 Japanese R2SP2 using Windows PXE boot, the target server is booting into a DOS Windows setup environment.The provisioning failure occurs due to the DOS Windows environment limitations.

Workaround: None

Agents

QCCR1D: 93940

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

Platform: Windows

Subsystem: Agents

Symptom: Missing `c:\windows\system32\ogshcap.dll` results in OGFS authentication failure to the Managed Server.

Workarounds:

- Uninstall the Windows Agent, reboot the system, and install a new Windows Agent

  or

- Enter one of the following commands based on your platform:

  x86_32

  ```
  C:\>copy "c:\Program Files\Opsware\agent\bin\ogshcap_x86.dll"
  c:\windows\system32\ogshcap.dll
  ```

  x86_64

  ```
  C:\>copy "c:\Program Files\Opsware\agent\bin\ogshcap_x64.dll"
  c:\windows\system32\ogshcap.dll
  ```

  IA64

  ```
  C:\>copy "c:\Program Files\Opsware\agent\bin\ogshcap_ia64.dll"
  c:\windows\system32\ogshcap.dll
  ```

  Restart the Agent.

Application Configuration

Bug ID: 137456 / QCCR1D: 48810

Description: Preserve format does not preserve comments when a comment exists on a line that has been deleted.

Platform: Independent

Subsystem: Application Configuration

Symptom: With preserve format enabled, any change to the value set that causes a line to be deleted from a configuration file will result in any comments on the deleted line to be removed also.

Workaround: None

Bug ID: 138610 / QCCR1D 49964

Description: Device Group Explorer not displaying inherited values correctly for servers which belong to multiple groups with identically named application configurations.

Platform: Independent

Subsystem: Application Configuration - Device Groups

Symptom: If two different device groups contain an application configuration that uses the same name, and each group has different values set for the configuration, and the same server belongs to both groups, then the Device Group Explorer will not show the proper inherited values when that server is displayed. It will only show the inherited values of the current device group in the browser and not both groups.

However, when you view the application configuration in the server's Device Explorer, you will see the value inheritance correctly.

Workaround: In general, if you want the application configuration instance of a server to be separate from the device group that the server belongs to, use a different name for each application configuration instance.

Bug ID: 139042 / QCCR1D: 50306

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

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rule

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

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

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

3 Select the Rule View tab

Bug ID: 158946 /QCCR1D: 70300 (see also 159963/71317)

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

Platform: Windows or Unix

Subsystem: Application Configuration Engine - Post Install Script

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

Workaround: Manually Restart WebLogic

QCCR1D: 83994

Description: Application Configuration aggregation fails when there are name space conflicts.

Platform: Independent

Subsystem: Application Configuration

Symptoms: If you specify certain values with conflicting namespaces in a valueset, it will effectively stop aggregation of sequences. For example, you have a sequence and a scalar value sharing a similar base namespace:

```
/namespace/key = "test"
/namespace/key/1 = "sequenceVal1"
/namespace/key/2 = "sequenceVal2"
```

This can also occur when you create a template with a scalar tag:

```
@cmlTag@
```

which sets that value, saves it, and then changes that tag to a sequence tag:

```
@*cmlTag@
@.@
```

Workaround: Locate where the conflict(s) occurs, and delete the conflicting value(s).

QCCR1D: 89554

Description: The addition of an application configuration instance fails with the error `java.sql.SQLException: ORA-20051: CANNOT UPDATE VIRTUAL_COLUMN_VALUES. RECORD IN CONFLICT WITH OTHER INSTANCES`.

Platform: Independent

Subsystem: Application Configuration

Symptom: If you attach an Application Configuration instance to a Server Group that contains a mix of servers from different cores in a Multimaster environment, a race condition that causes Multimaster conflicts can occur when you attempt to perform an Application

Configuration operation (for example, scan/push) on the Server Group. It also deletes the Application Configuration instance from the Server Group as soon as the job finishes. This condition occurs only during a small time window, before database updates are synchronized.

Workaround: Resolve all transaction conflicts on the server that performs the Application Configuration instance delete.

Bug ID: 88909

Description: filename-key values are not inherited in referenced templates when the value is left as the default.

Subsystem: Application Configuration/SA Client

Symptom: When referencing a filename-key value in an application configuration or a post-install script, the value does not get populated from the filename-default. However, if you set the value in any scope, it does show up.

Description: If you create an AppConfig template, or an AppConfig post-install script, and leave the filename-default value as default, the template or post-install script will not be able to find the referenced file in the namespace.

The filename-key is the location in namespace where the name of the target configuration file is stored. If the filename-key for a configuration file is `/files/configFile`, then any template that uses the tag `@/files/configFile@` is asking that tag be replaced with the location of the pushed file.

Failing to set this value results in the AppConfig being unable to find the target configuration file path.

Workaround: Specify the Filename value in the Application Configuration properties at any inheritance level. For example, open the Application Configuration, select the Default Values tab, and then set the filename path for the target configuration filename.

Audit and Remediation

Bug ID: 137901 / QCCR1D: 49255

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

Platform: Independent

Subsystem: Audit and Remediation - Application Configuration Rules

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

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

QCCR1D: 92288

Description: Registered Software rule: Value-based checks functionality seems to be broken.

Platform: Solaris

Subsystem: Audit and Remediation

Symptom: Value-based check audits are not supported for Solaris patches: since the `install_condition` field is currently not available as an auditable field, value-based audit checks fail.

Workaround: Use the Solaris patch name for audits instead of the version (the name contains the version).

QCCR1D: 94011

Description: Compliance calculation of hardware rules is incorrect after upgrade.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: After upgrade from SAS 7.x to SA 7.80, hardware rules in the pre-SA 7.80 format do not calculate the compliance status correctly wherever compliance status is shown. This includes the **Summary Page** in the Audit Results browser, the Dashboard, the Compliance Status page in the Server Browser, and in the Compliance Reports.

Workaround: Resave the audit, audit policy, or snapshot specification with the hardware rules and rerun the job.

QCCR1D: 94106

Description: Remediating AIX packages fails if a preview is run before starting the job.

Platform: Independent

Subsystem: Audit and Remediation

Symptom: Under certain circumstances, performing a preview when installing, removing or, remediating AIX software can cause the subsequent steps of the job to fail immediately or provide a false positive.

Workaround: After performing the preview, close the job window. Start the job again but skip the preview step.

Content Migration

Bug ID: 80628

Description: Content Migration Issue with Some Custom Search Parameters

Platform: Independent

Subsystem: Content Migration from SA 7.50 to SA 7.80 - SA Client/Search/Custom Attributes

Symptom: During an upgrade from SA 7.50 to 7.80, some saved dynamic group search parameters for custom fields cannot be migrated correctly. This is due to an issue with migrating the custom fields used in SA Client advanced searches. If you have a saved search/dynamic group rule containing two or more custom field search rules that are combined without proper grouping, then those search rules cannot be migrated during system upgrade.

Workaround: None. You must recreate the search parameters.

Content Upload

Bug ID: 88909

Description: A stale NFS file handle error occurs during content upload.

Subsystem: Content Migration

Symptom: During the fresh install or upgrade content upload phase or when importing a package or patch into the SA Client Library (or using the OCLI), a package or its signature file may not be copied to its destination due to a stale NFS file handle.

As a result, although the SA considers the upload successful, the file, or its `.sig` file, is missing in the Software Repository.

Workaround:

If the stale NFS File Handle error occurs during an install or upgrade content upload:

1. Find and remove the package in the SA Client Library, or use UAPI UnitService.remove() to delete the reference to the non-existing package.
2. Re-run the content upload which should upload the missing package.

If you rerun the content upload but do not delete the package first:

1. Find and remove the package in the SA Client Library, or use UAPI UnitService.remove() to delete the reference to the non-existing package.
2. 2. Check if the file `/tmp/tmpXXXX.sh` still exists. If so, find the script that corresponds to the upload failure, and then use the upload command to re-upload the package.
3. If no `tmp` file exists, find the upload command in the upload `.conf` file.

For individual upload failure due to NFS stale file handle:

1. Find and remove the package in the SA Client Library, or use UAPI UnitService.remove() to delete the reference to the non-existing package.

DCML Export Tool (DET)

Bug ID: 138949 / QCCR1D: 50303

Description: Some imports fail if Microsoft patches are missing.

Platform: Windows

Subsystem: DCML Export Tool (DET)

Summary: By design, DET doesn't allow the import of Microsoft patches; they must be inserted into SA by the MS patch database import process. Thus, if an export contains a Microsoft patch and the destination mesh is not up-to-date with regard to MS patches, the import will not import the missing patches. It will print a warning at the end like this:

```
The following Windows patches were not uploaded:
Q911564 (WindowsMedia-KB911564-x86-ENU.exe)
```

The behavior described in the preceding paragraph is not a bug. However, associated objects in the failed import will not be imported as a side effect. For example, if you import a folder or a device group with multiple attachments (such as software policies or OS sequences) and the import also contains a Windows patch that does not exist in the destination mesh, then the import fails and the attached objects are not imported.

Workaround: Import MS patches with the SA Client feature that relies on the MS patch database. Then, you can import the other objects (such as software policies) with DET.

Bug ID: 135494 / QCCR1D: 46848

Description: Import correctly detaches and deletes objects, but preview incorrectly states that the objects will be renamed.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Summary: Here's an example scenario where this problem occurs:

1. Create a template with two applications in it. Export this from Mesh A and import into Mesh B.
2. Detach one application from the template and incrementally export with the `-del` argument. This export will contain the detachment and the deletion of the application.
3. Preview the import with the `-del` argument, then perform the import with `-del` argument.

In this scenario, the preview incorrectly shows that the application will be renamed because it is in use by a template. The actual import will correctly delete the application. This problem also occurs when other objects are detached and deleted, for example, `app/package`, `app policy/app policy`, and so on.

Note that this problem does not occur if *both* objects are being deleted, only if one object is being deleted and detached from the other.

Workaround: None

Bug ID: 158971 /QCCR1D: 70325

Description: Export to delete an audit policy with server module rule shouldn't mark server module related packages and policies deleted.

Platform: Independent

Subsystem: DET Export Folder Filter/Audit and Remediation/SMO

Symptom: If you attempt to export a folder that contains audit policies which reference Software Discovery server module, and then perform another export of that same folder as a baseline and add the delete command to remove the audit policies. all Software Discovery objects referenced by the audit policies will be renamed.

Workaround:

In order to maintain all Software Discovery objects that are referenced in an audit policy, create a folder that contains all of the same Software Discovery objects, and then export that folder. After you import the audit policy folder into a target core, then import the folder containing the Software Discovery objects.

QCCR1D: 90725

Description: Cannot export Software Policies using CBT/DET.

Platform: Independent

Subsystem: DCML Export Tool (DET)

Symptom: Cannot export Software Policies by themselves using CBT; you must export the folder that contains the software policy.

Workaround: The `FolderFilter` filter type has been extended. Its `<path> attribute`, which previously only allowed a folder pathname, has been extended to allow a pathname for any exportable type that lives in folders. These types include folders, OS sequences, scripts, packages, software policies, and audit policies. The optional `<recursive> FolderFilter` attribute only makes sense for folders, so it must be left out or set to `No` when exporting any non-folder object. Some examples are provided below:

Export a folder recursively:

```
<FolderFilter rdf:ID="f1">
    <path>/data/folder1</path>
    <recursive rdf:resource="&filter;Yes" />
  </FolderFilter>
```

Export a single software policy:

```
<FolderFilter rdf:ID="swp1">
    <path>/data/folder2/rhel5 policy</path>
  </FolderFilter>
```

Export a single package:

```
<FolderFilter rdf:ID="p1">
    <path>/data/folder3/php-4.4.7-Win32.zip</path>
  </FolderFilter>
```

Device Explorer

Bug ID: 167668 / QCCR1D: 79022

Description: Browsing IIS Metabase objects in Device Explorer on Windows 2008 Server throws exceptions and objects are unreadable.

Platform: Windows Server 2008

Subsystem: Device Explorer/Audit Rules

Symptom: If you browse a Windows 2008 x86 managed server's Windows IIS Metabase inside the SA Client, either in the Device Explorer or the Audit or Snapshot window, you will not be able to see the metabase objects because Windows IIS 7.0 does not use the metabase to store configuration data. Rather, Windows IIS 7.0 uses XML configuration files to display data, which is currently not supported.

Workaround: From a command prompt on the Windows 2008 managed server, run the following command, which will install Microsoft's compatibility layer to make some IIS configuration objects available to SA.

```
servermanagercmd -i web-metabase
```

Note that this compatibility layer is known not to support all available IIS 7.0 configuration entries. In addition, some IIS 6.0 entries are deprecated. Please consult the MSDN documentation on IIS 7.0's metabase compatibility layer for details.

Bug ID: 154416 / QCCR1D: 65770

Description: Unable to add registry key HKEY_CURRENT_USER to the Library

Platform: Windows

Subsystem: Device Explorer

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

“Certain content cannot be captured...”.

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

Extensible Discovery

QCCR1D: 94059

Description: A package removed from the Customer Provided Scripts policy is not uninstalled.

Subsystem: Extensible Discovery

Platform: Independent

Symptom: Remove a package from the Customer Provided Scripts policy then run Extensible Discovery. The package is not removed from the server because the remediation job is not triggered.

Workaround: Add a package to the policy, or change the name of one of the packages in the policy. A remediation will be kicked off the next time extensible discovery is run, and the packages removed from the policy will be uninstalled from the server(s).

Gateways

Bug ID: 147215 / QCCR1D: 58569

Description: Uninstallation of the core gateway does not remove certificates.

Subsystem: Gateways

Platform: Independent

Symptom: When the core Gateway is uninstalled using the SA Installer on a SA core, it does not remove the data under /var/opt/Opsware/crypto/opswgw-cgw0-<DCNAME>. This can cause a problem if the core is reinstalled with a different crypto database because the certificates will no longer be valid.

Workaround: Remove old Gateway crytpo files.

Global Shell

Bug ID: 129237 / QCCR1D: 41396

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

Subsystem: SA Client - Remote Terminal, Global Shell

Platform: Independent

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

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

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

QCCR1D: 88158

Description: hub can't start after upgrading kernel on Red Hat Enterprise Linux 4.7 to stop kernel panics.

Subsystem: Global File System - Hub

Platform: Red hat Linux

Symptom: After a Red Hat kernel is upgraded to 4.7, certain Global File System components cannot be rebuilt due to missing dependencies.

Workaround: Upgrade to `kernel-smp-2.6.9-78.0.13` and install `kernel-smp-devel-2.6.9-78.0.13`.

Bug ID: 129501 / QCCR1D: 41613

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

Subsystem: SA Client - Global Shell

Platform: Linux

Symptom: In a Global Shell session, change the encoding with the swenc command. Background processes that are running in the Global Shell session might fail.

Workaround: Wait until background processes have completed before changing the encoding with swenc.

Bug ID: 130514 / QCCR1D: 42395

Description: User must belong to Administrators group to browse metabase.

Subsystem: SA Client - Global Shell

Platform: Windows

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

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

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

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

Bug ID: 133316 / QCCR1D: 44670

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

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

Subsystem: Global Shell

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

For example:

```
$ pwd
/opsw/Server/@/m229/files/Administrator/
$ cd c
$ ttlg -l Administrator dir c:\\
ttlg: Error getting current directory (1161): No such file or directory
$ cd ../C
$ ttlg -l Administrator dir c:\\
```

```
Volume in drive C has no label.
Volume Serial Number is 6836-A79C
```

Workaround: Users must observe file system case even when they change into Windows server file systems. This is made easier if they use the tab completion features of their shells.

Bug ID: 137948 / QCCR1D: 49302

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

Platform: Independent

Subsystem: Global File System

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

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

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

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

Bug ID: 140696 / QCCR1D: 52050

Description: In rosh, an interactive Windows program hangs.

Platform: Windows

Subsystem: Global Shell

Symptom: Launch a Global Shell session, rosh on a Windows managed server, run an interactive program such as `ismtool`. The interactive program will hang.

Workaround: None, unless you have access to the source code of the Windows interactive program. To fix the code, for example in Python, call the `sys.stdout.flush()`.

Bug ID: 142089 / QCCR1D: 53443

Description: Invalid argument error when browsing Windows IIS Metabase by user that does not belong to server's Windows Administrator's group

Platform: Windows

Subsystem: Global Shell

Symptom: If a user is browsing a Window's server's IIS Metabase, and that user does not belong to the Windows Administrator's group on that server, the user will get an "invalid argument" error. The user will also not be able to see any metabase objects.

Workaround: Add the user to the target server's Administrator group.

Bug ID: 143198 / QCCR1D: 54552 (see also 42545/130717)

Description: OGFS installation fails if the `hugemem` kernel is installed.

Platform: Linux

Subsystem: Global File System - backend

Symptom: OGFS installation fails if the `hugemem` kernel is installed.

Workaround: Log on as root to the OGFS server and enter the following commands:

```
cd /usr/src/
ln -s linux-2.4.21-47.EL linux-2.4.21-47.ELhugemem
```

Then, run the SA Installer again to install the OGFS.

Bug ID: 145833 / QCCR1D: 57187

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

Platform: Independent

Subsystem: Global File System

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

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

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

Bug ID: 148571 / QCCR1D: 59925

Description: Cannot copy read-only files to a managed server using the OGFS.

Platform: Independent

Subsystem: Global File System - backend

Symptom: When using the OGFS to copy read-only files to the file system of a managed server as a non-root user, `cp` may return a `Permission denied` error. The target file will be created but will be empty.

Example:

```
$ pwd
/opsw/Server/@/server-1/files/non-root/tmp
$ echo abc > abc
$ chmod -w abc
$ ls -l abc
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
$ cp abc ABC
cp: cannot create regular file `ABC': Permission denied
$ ls -l abc ABC
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
-r--r--r-- 1 59820 1 0 2007-05-08 23:01 ABC
```

Workaround: After the cp command fails, make the target file writable, retry the cp command, and then make the file read-only after the copy is completed. Example:

```
$ ls -l abc ABC
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
-r--r--r-- 1 59820 1 0 2007-05-08 23:01 ABC
$ chmod +w ABC
$ cp abc ABC
$ ls -l abc ABC
-r--r--r-- 1 59820 1 4 2007-05-08 23:00 abc
-rw-r--r-- 1 59820 1 4 2007-05-08 23:01 ABC
$ chmod -w ABC
```

QCCR1D: 92865

Description: A Slice Component bundle upgrade fails due to I/O errors to /var/opt/opsware/ogfs/mnt/root/opsw

Platform: Solaris

Subsystem: Global File System/Shell Backend

Symptom: On Solaris hosted SA cores, if the hub process terminates before the OGFS is unmounted, attempting to unmount the OGFS (including trying to stop the hub with the command
/etc/init.d/opsware-sas stop hub will result in a Device Busy error.

The usual opsware-sas start/stop script will unmount before stopping the hub process, so under ordinary circumstances, this problem will not manifest. It will occur only if the hub terminates. unexpectedly.

Workaround: Restart the affected server.

Jobs and Sessions

Bug ID: 139762 / QCCR1D: 51116

Description: Different IDs are shown for the same job on NGUI and OCC web.

Subsystem: Jobs and Sessions

Platform: Independent

Symptom: You schedule the installation of a patch on a server to run at a later time. The job is assigned different IDs in the NGUI and the OCC. The Oracle view TRUTH.JOBS is also affected.

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

Workaround: None

Manage Boot Client (MBC) Tool

QCCR1D: 93593

Description: Core upgrade from SA 7.50 to 7.80 deletes the MAC link created using MBC in 7.50.

Subsystem: Manage Boot Client (MBC) Tool

Platform: Independent

Symptom: If server records were created using MBC in SA 7.50 but the servers were never powered on to register themselves with the Core, after the 7.50 core is upgraded to SA 7.80, the MAC links of these server records are deleted from the following boot server's directory:

`/opt/opsware/boot/tftpboot/pxelinux.cfg/`

Workaround: None

QCCR1D: 93597

Description: `configureAutomaticProvisioningRule()` should initiate jobs as the user who ran the UAPI call.

Subsystem: Manage Boot Client (MBC) Tool

Platform: Independent

Symptom: MBC OS Provisioning jobs are initiated by the user `detuser`. Therefore, in order to view the progress and results of the job, the original user must have the `view all jobs` permission, which raises security issues. Also, because the job runs as the user `detuser`, it has access to all software policies, including some that the original user may not have had access to and potentially could install sensitive information onto the server that they control.

Workaround: None

QCCR1D: 93598

Description: Itanium OS Provisioning cannot be done automatically using MBC.

Subsystem: Manage Boot Client (MBC) Tool

Platform: Independent

Symptom: Itanium OS Provisioning fails because IA64 uses eLilo boot which MBC does not yet support.

Workaround: None

QCCR1D: 93600

Description: In a mesh with large Facility and server data, MBC took several minutes to process input.

Subsystem: Manage Boot Client (MBC) Tool

Platform: Independent

Symptom: Running MBC in Facilities with a large amount of server data may take a long time.

Workaround: None

QCCR1D: 93602

Description: MBC is not localized.

Subsystem: Manage Boot Client (MBC) Tool

Platform: Independent

Symptom: The drop down box values in MBC's Single Client Form and all values the user attempts to create using CSV format, such as value of custom attributes `Customer`, `AdminPassword`, `ComputerName`, and so on are not localized.

Workaround: None

Model Repository

Bug ID: 138694 /QCCR1D: 50048

Description: Upgrade failed due to an Oracle database problem.

Subsystem: Model Repository

Platform: Independent

Symptom: Oracle has a SYS.AUDIT_ACTIONS table. Oracle's default synonym AUDIT_ACTION is for SYS.AUDIT_ACTIONS. When the Model Repository creates the TRUTH.AUDIT_ACTIONS table, the synonym is changed to TRUTH.AUDIT_ACTIONS. When you upgrade Oracle software, Oracle will recreate the synonym as SYS.AUDIT_ACTIONS.

Workaround: If the AUDIT_ACTIONS synonym is overwritten by an Oracle upgrade, enter the following commands:

```
Su - oracle
Sqlplus "/ as sysdba"
Grant create session to truth;
Connect truth/<password>

Create or replace public synonym audit_actions for audit_actions;
```

QCCR1D: 91960

Description: `Checkpoint not complete` error found in Oracle 10g `alert.log`.

Subsystem: Model Repository

Symptom: A `checkpoint not complete` error occurs when Oracle attempts to reuse a log file but the checkpoint that flushes the blocks that may have redo in this log file has not yet completed. Oracle must wait until that checkpoint completes before it can reuse that file. During this time (while Oracle cannot allocate a new log) processing is suspended in the database.

This error can appears in the alert log many times a day or only occasionally. The possible solution is to eliminate I/O bottlenecks, or to compensate for a slow I/O subsystem.

Workaround: There are several possible solutions:

- Put your redo logs on faster disks.
- Add additional redo logs. To do so, use the following syntax:

  `# su - oracle`

  `# sqlplus "/ as sysdba"`

  `SQL> select * from v$logfile;` (sql will show location of redo logs)

  `SQL> select * from v$log;` (GROUP = redo logs group no, BYTES = size of redo logs,)

  For example, to add a new redo group with two members (you may need to change directory and file names):

  ```
  SQL> ALTER DATABASE ADD LOGFILE GROUP 4 ('/u02/oradata/truth/log4a.log',
  '/u03/oradata/truth/log4b.log') SIZE 32M;
  ```

- Increase the size of redo logs
- Increase the number of db writer processes
- Adjust `fast_start_mttr_target.`

NA/SA Integration

QCCR1D: 84382

Description: NA - SA integration requires extra steps

Platform: Independent

Subsystem: NA/SA Integration

Symptom: Logging into the SAS Web Client generates a pop-up stating that the NA server cannot be contacted. Attempting to log into NA with an SA account generates an invalid user name or password error even though NA has been set up for SA authentication, `twist.nasdata.host` is specified correctly in the `twist.conf file`, both the Web Services Data Access Engine (`twist`) and the NA server have been restarted, and the `.jar` files have been downloaded and seem to be in the correct location on each server.

Workaround: Comment out (or delete) the three lines in `server/ext/wrapper/conf/jboss_wrapper.conf` below:

```
#Following are added for bug 150387

#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
```

Since SAS 7.8 does not use Java 1.4.2, those lines are no longer needed.

Online Help

QCCR1D ID: 91567

Description: Online Help Search Results Sometimes Blank when Scrolling Results Using Mouse Wheel

Platform: Independent

Subsystem: SA Client/SAS Web Client - Online Help Search

Symptom: When using the SA Client or SAS Web Client online help search tool, sometimes the results pane will appear to be blank when using a mouse wheel while scrolling the results.

Workaround: Click inside the search results on any topic and the original search list will appear, and do not use your mouse wheel to scroll online help search results.

Oracle/SA

QCCR1D: 88319

Description: An Oracle result set error causes incorrect **Patches recommended by Vendor** patch list in the SAS Web Client.This defect should affect on manually installed Oracle 11g databases for the Model Repository. This patch is already part of the HP-supplied Oracle database.

Platform: Independent

Subsystem: Oracle/SA Model Repository

Symptoms: When you launch the SAS Web Client, select a Managed Server, and filter it for patches, then go to **Patches recommended by Vendor**, no patches are displayed.

Workaround: Apply Oracle Bug Patch 8300752.

QCCR1D: 93744

Description: `ORA-00700: soft internal error, arguments: [kesqsMakeSql-invstat:elpsTime]` in `alert.log` file.

Platform: Linux/Solaris

Subsystem: Oracle/SA Model Repository

Symptoms:

1. The `from alert_truth.log` (`/u01/app/oracle/diag/rdbms/truth/truth/trace/alert.log`) lists errors that are similar to the ones listed below:

```
...
Sun May 10 13:00:21 2009
Errors in file /u01/app/oracle/diag/rdbms/truth/truth/trace/
truth_j002_31530.trc (incident=131514):
ORA-00700: soft internal error, arguments:
[kesqsMakeSql-invstat:elpsTime], [], [], [], [], [], [], []
```

```
Incident details in: /u01/app/oracle/diag/rdbms/truth/truth/incident/
incdir_131514/truth_j002_31530_i131514.trc
```

2 In addition to the errors in `alert.log` file, there are also `cdmp_*` files in the `/u01/app/oracle/diag/rdbms/truth/truth/trace` directory. The `cdmp` files will be similar to the ones shown below:

```
drwxr-xr-x 2 oracle oinstall 20480 May 10 13:00 cdmp_20090510130051
drwxr-xr-x 2 oracle oinstall 20480 May 10 13:00 cdmp_20090510130056
drwxr-xr-x 2 oracle oinstall 20480 May 10 13:01 cdmp_20090510130100
drwxr-xr-x 2 oracle oinstall 20480 May 10 13:01 cdmp_20090510130104
drwxr-xr-x 2 oracle oinstall 20480 May 10 13:01 cdmp_20090510130108
```

Each `cdmp` directory will include several trace files.

3 The trace files will include text which is similar to:

```
========= Dump for incident 131514 (ORA 700
[kesqsMakeSql-invstat:elpsTime]) ========

*** 2009-05-10 13:00:21.274
----- Current SQL Statement for this session (sql_id=6jbrg916bjmqc) -----
DECLARE job BINARY_INTEGER := :job; next_date TIMESTAMP WITH TIME ZONE :=
:mydate; broken BOOLEAN := FALSE; job_name VARCHAR2(30) := :job_name;
job_subname VARCHAR2(30) := :job_subname; job_owner VARCHAR2(30) :=
:job_owne
r; job_start TIMESTAMP WITH TIME ZONE := :job_start; job_scheduled_start
TIMES
TAMP WITH TIME ZONE := :job_scheduled_start; window_start TIMESTAMP WITH
TIME Z
ONE := :window_start; window_end TIMESTAMP WITH TIME ZONE := :window_end;
BEGI
N DECLARE
ename VARCHAR2(30);
BEGIN
ename := dbms_sqltune.execute_tuning_task(
'SYS_AUTO_SQL_TUNING_TASK');
END; :mydate := next_date; IF broken THEN :b := 1; ELSE :b := 0; END IF;
END;

----- PL/SQL Stack -----
----- PL/SQL Call Stack -----
object line object
handle number name
0xb5c20750 7294 package body SYS.DBMS_SQLTUNE_INTERNAL
0xb5272030 8 SYS.WRI$_ADV_SQLTUNE
0xc393d620 545 package body SYS.PRVT_ADVISOR
0xc393d620 2597 package body SYS.PRVT_ADVISOR
0xc3953d90 241 package body SYS.DBMS_ADVISOR
0xc3521f18 702 package body SYS.DBMS_SQLTUNE
0xb5bb4e68 4 anonymous block

----- Call Stack Trace -----
calling call entry argument values in hex
location type point (? means dubious value)
-------------------- -------- --------------------
----------------------------
skdstdst()+28 call kgdsdst() 000000000 ? 000000000 ?
```

```
ksedst1()+95 call skdstdst() 000000000 ? 000000000 ?
ksedst()+35 call ksedst1() 000000000 ? 000000001 ?
dbkedDefDump()+1105 call ksedst() 000000000 ? 000000001 ?
ksedmp()+35 call dbkedDefDump() 000000003 ? 000000002 ?
__PGOSF52_ksfdmp()+ call ksedmp() 000000003 ? 000000002 ?
dbgexPhaseII()+287 call __PGOSF52_ksfdmp() 000000003 ? 000000002 ?
dbgexProcessError() call dbgexPhaseII() 2B11F74EB6D0 ? 2B11F787B710 ?
dbgeExecuteForError call dbgexProcessError() 2B11F74EB6D0 ? 2B11F787B710 ?
dbgePostErrorKGE()+ call dbgeExecuteForError 2B11F74EB6D0 ? 2B11F787B710 ?
dbkePostKGE_kgsf()+ call dbgePostErrorKGE() 0096FA1E0 ? 2B11F7910040 ?
kgeadse()+392 call dbkePostKGE_kgsf() 0096FA1E0 ? 2B11F7910040 ?

Cause:
Oracle bug number:
Bug 7025700: -> Marked as duplicate of bug 8224438
Bug 7757533: -> Marked as duplicate of bug 8224438
Bug 8224438: -> Marked as duplicate of bug 7643188
```

Workaround: Contact Oracle Support to verify that you are experiencing same bug.Oracle Support has recommended applying patch: 7643188.

Operating System Provisioning

Bug ID: 133894 / QCCR1D: 45248 (see also 143395/54749)

Description: `Wordbot` error during import media.

Subsystem: OS Provisioning - `import_media` Utility

Platform: Independent

Symptom: There appears to be a bug in the mechanism that connects to the Data Access Engine, and retrieves and then caches customer information associated with the IP address of the request to the Software Repository server. Occasionally, this results in a `wordbot.accessDenied` error.

Workaround: None. This error is caused by a transient problem within the Software Repository. The `import_media` script will retry each package upload three times, which is normally sufficient to work around this issue. If you see this message logged frequently and the affected package is not correctly uploaded even with the retries, contact support.

Bug ID: 144615 / QCCR1D: 55969

Description: Unable to save the change of OS Sequence Remediation's Script Timeout using Save Changes dialog

Platform: Independent

Subsystem: OS Provisioning - OS Sequence with Remediation

Symptom: If you create an OS Installation Profile, and in the Remediate Policies task object, enable remediation, and in an Ad-Hoc Script set a Script Timeout value, the timeout value will be saved when you close the OS Sequence and click Yes to save changes, or if you use the **File menu ➤ Save** function.

However, if after you save this initial configuration you open the OS Sequence again and make a change to the script timeout value, and then attempt to close the OS Sequence, you will be prompted to save the changes in a dialog. If you click Yes, the changes will not be saved.

Workaround: During OS Sequence modification phase, in order to save your changes to the Script Timeout field in an Remediate Policies object, click the mouse to empty boxes (such as Command box) to make the OS Sequence object window dirty. The changes would then be saved through either methods (through File menu ➤ Save, or close the OS Sequence Window and choose Yes to save).

Bug ID: 143459 / QCCR1D: 54813

Description: If you provision a server that has customer “Not Assigned”, and it got assigned a customer during provisioning, then you changed the server's customer back to “Not Assigned”, it caused an error.

Platform: Any

Subsystem: OS Provisioning/Customer Assignment

Symptom: If you provisioned a sever that had a customer assignment set to “Not Assigned”, and then provision the server with an OS Profile or OS Sequence that has a customer the server will be assigned to the customer set in the OS Profile or OS Sequence. However, if you attempt to change the server's customer assignment back to “Not Assigned”, you get an error. Not Assigned is an invalid customer assignment post-provisioning.

Workaround: None

Bug ID: 146003 / QCCR1D: 57357

Description: Release Note Additional packages on OS node not installed in 6.x.

Platform: Unix

Subsystem: OS Provisioning

Symptom: Scenario:

1. Create a Linux or Solaris OS Installation Profile.
2. Attach additional packages to the OS Installation Profile (either in the **Prepare OS Wizard** or later on the **Packages** tab).
3. Attach the OS Installation Profile to an OS Sequence.
4. Provision a server with the sequence

When this provisioning occurs, any additional packages (beyond what Jumpstart/Kickstart will install based on your profile) will *not* be installed when provisioning using an OS Sequence, whereas legacy OCC Web provisioning will install them.

Workaround: None

Bug ID: 148335 / QCCR1D: 59689

Description: Not able to provision an ESX3 VM with 2 NICs via DOS image.

Platform: Windows 2003

Subsystem: OS Provisioning

Symptom: VMware guests with more than one network interface cannot connect in DOS boot image with native network drivers.

When network booting a VMware guest machine via the DOS boot image (the **windows** option at the PXE menu), if the guest has more than one virtual network adapter configured, an error message will display and the machine will not be able to enter the unprovisioned server list correctly.

Workaround: Boot with the WinPE boot image. Alternately, perform provisioning with only one network adapter configured and add additional adapters after OS provisioning.

Bug ID: 157913 / QCCR1D: 69267

Description: Invalid `base_packages` value leads to unclear error message.

Subsystem: OS Provisioning

Platform: Independent

Symptom: When running an OS Sequence on a server where the specified `model_base_packages` value is invalid, the OS Provisioning job completes successfully. However, the `base_packages` Software Policy is not created and no error message is displayed.

Workaround: Specify a valid `model_base_packages` value and run the OS Sequence again.

QCCR1D: 92612

Description: When using the SA Client **Prepare OS** wizard, **Define Installation** tab after selecting the Windows Server 2008 platform, the option of a DOS-based installation is displayed as the default.

Subsystem: OS Provisioning

Platform: Windows Server 2008

Symptom: When using the **Prepare OS** wizard, **Define Installation** tab, the DOS option is shown as the default when defining a Windows Server 2008 profile. A DOS-based installation is not a valid option for Windows Server 2008. If DOS is selected, OS Provisioning jobs using this profile may fail.WINPE is the only valid installation type for Windows Server 2008 installations.

Workaround: Use the In the **Prepare OS Wizard ➤ Define Installation** tab, select WINPE for the **Select Installation Type** option.

QCCR1D: 89928/93573 /93592

Description: If the Slice Component bundle fails or is uninstalled, OS Provisioning fails even though Build Managers on other Slices hosts are still running.

Platform: Independent

Subsystem: OS Provisioning

Symptom: When a Slice Component bundle is uninstalled, the `dhcp.conf` file is not updated to point to another Slice. Therefore, OS Provisioning fails.

Workaround: Before you uninstall a slice, ensure that the OS provisioning components (specifically the DHCP server and the PXE/TFTP server) do not depend on the slice. Check the DHCP server's configuration file (`/etc/opt/opsware/dhcpd/dhcpd.conf`) and the PXE server's configuration file (`/opt/opsware/boot/tftpboot/pxelinux.cfg/default`) to see if there are references to the slice's IP, and if so, change the IP value to a known, good slice. Then restart the DHCP server.

QCCR1D: 93214

Description: When creating a VM and performing OS Provisioning, no live log details are shown in the
Job window.

Platform: Independent

Subsystem: OS Provisioning

Symptom: When attempting to create a VM with OS Provisioning, you may find that no live installation details are displayed in the job window.

Workaround: When the operating system installation completes, the Job window is updated with the live log details.

QCCR1D: 93579

Description: If you run `import_media` in Satellite with the argument `upload=yes` and with the `--folder` option specified to a non-default folder, exceptions occur.

Platform: Independent

Subsystem: OS Provisioning

Symptom: From an SA Satellite, when you launch the `import_media` utility to import media with the `--upload=yes` argument (or you do not specify the upload option) and with the `--folder` option specified to a non-default folder, exceptions occur.

Workarounds:

1. Run `import_media` from the Satellite specifying `upload=no`.
2. Run `import_media` from the satellite specifying `upload=yes`, but do not specify the `--folder` option.

QCCR1D: 93583

Description: A Build Customization Script imported as a multi-platform package cannot be added to an OS Profile.

Platform: Independent

Subsystem: OS Provisioning - Build Customization Scripts

Symptom: If you import a Build Customization Script with more than one platform ID selected for the import, you will not be able to add the Build Customization Script to an OS Profile.

Workaround: None

QCCR1D: 93585

Description: Content of Build Customization Script is not internationalized.

Platform: Independent

Subsystem: OS Provisioning - Build Customization Scripts

Symptom: If the content of a Build Customization Script contains non-ASCII characters, these characters are not correctly internationalized.

Workaround: None

QCCR1D: 93782

Description: Linux reprovisioning becomes interactive if the value for `truth.dcName` 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.dcName` 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.

Workaround: None

QCCR1D: 93833

Description: OS Provisioning fails if GMT time zone is specified in the Kickstart configuration file under Red Hat Enterprise Linux 5.3.

Platform: Red Hat Linux

Subsystem: OS Provisioning

Symptom: Under Red Hat Enterprise Linux 5.3, OS Provisioning fails if you attempt to specify the time zone in an OS Profile's `ks.cfg` file in any of the following formats:

```
timezone --utc Etc/GMT
timezone --isUtc GMT
timezone --isUtc Etc/GMT
```

Workaround: See the instructions provided by Red Hat at:

https://bugzilla.redhat.com/show_bug.cgi?id=481617

QCCR1D: 102965

Description: An SA Core upgrade from SA 7.50 to SA 7.80 loses any MAC links created using the Master Boot Client (MBC).

Platform: Independent

Subsystem: OS Provisioning

Symptom: If you have created pre-defined unprovisioned devices (PUDs) using the Master Boot Client under SA 7.50, then upgrade the core to SA 7.80 with the PUDs powered down, any MAC links in the PUD specification are lost although the PUDs are listed in the SA Client.

Workaround: None

Patch Management for Solaris

QCCR1D: 88516

Description: When you install a Solaris patch or patch cluster and the install job generates a large amount of output, the first part of the output may be truncated.

Platform: Solaris

Subsystem: Patching

Symptoms: When you run a job in the SA Client to install Solaris patches, select the Job Status window, select the Output tab and scroll to the top of the window, the displayed output is missing some information at the top.

Workaround: None.

QCCR1D: 89123

Description: If the solpatch_import utility is unable to download patches through your firewall, check to make sure the firewall allows the user-agent “Wget/1.9.1”.

Platform: Solaris

Subsystem: Patching - solpatch_import utility

Symptoms: When you attempt to use the solpatch_import utility to download patches, your firewall disallows it.

Workaround: Make sure your firewall allows the user-agent “Wget/1.9.1”.

QCCR1D: 91914

Description: When a Solaris patch installation fails because the Solaris server does not have enough disk space, the resulting message is unclear.

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: When you install a patch on a Solaris system and the patch installation fails because the Solaris server does not have enough disk space, a message like the following is displayed (emphasis added).

```
Cause: com.opsware.common.LegacyException
Exception Message: Summary: An error occurred while installing or removing
this package.
Detail: An error occurred while installing or removing this package. The
package may not be applicable for the selected server.
```

```
Resolution Steps: Verify that the package is correctly defined and applicable
for the selected server. If the problem persists, please contact technical
support.
Legacy Error Code: cogbot.packageError
$OpswareError= cogbot.packageError command= /opt/opsware/agent/bin/unzip -qd
/var/opt/opsware/agent/remediate_pkgs0/10_x86_Recommended.zip1239282053.5 /
var/opt/opsware/agent/remediate_pkgs0/10_x86_Recommended.zip < /dev/null
package= /var/opt/opsware/agent/remediate_pkgs0/10_x86_Recommended.zip
results= Could not expand file: /var/opt/opsware/agent/remediate_pkgs0/
10_x86_Recommended.zip1239282053.5/10_x86_Recommended/120012-14/SUNWckr/
reloc/kernel/sys/pset: write error (disk full?). Continue? (y/n/^C)
warning: /var/opt/opsware/agent/remediate_pkgs0/
10_x86_Recommended.zip1239282053.5/10_x86_Recommended/120012-14/SUNWckr/
reloc/kernel/sys/pset is probably truncated
```

Workaround: Compare the message to the message above to determine if disk space is the problem. To install the patch, make more disk space available on the Solaris server.

QCCR1D: 92231

Description: Install Software fails to install a Solaris patch cluster due to time out.

Platform: Independent

Subsystem: Solaris Patch Management

Symptom: The default timeout for installing a package is 1 hour. However Solaris patch clusters typically take longer than 1 hour to install.

Workaround: To increase the timeout value follow these steps:

1. Log into the SA Web Client as a user who has permission to do **System Configuration**.
2. From the **Navigation** panel, under **Administration**, select **System Configuration**.
3. From **Opsware ➤Select a Product**, select **Command Engine**.
4. Find the parameter `way.remediate.package_alarm_timeout` and set the value to 18000 (5 hours).
5. Click **Save**.

This new timeout value should provide sufficient time to install a Solaris patch cluster.

QCCR1D: 93095

Description: Installing Deferred-Activation Patches on Solaris systems sometimes reports incorrect results.

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: When you install a Deferred-Activation Patch on a Solaris system, the patch job sometimes reports that the patch installation succeeded when it actually failed, and it sometimes reports that the patch installation failed when it actually succeeded.

Workaround: Examine the detailed output messages from the patch installation job to determine the actual patch installation results. For example, the detailed messages may indicate that the patch was not installed because it was already installed.

QCCR1D: 93165

Description: Install cluster job fails in the middle of installation because a patch requires an immediate reconfiguration reboot.

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: During a cluster installation, a patch can require an immediate reconfiguration reboot, but the reboot cannot occur causing the cluster installation to fail.

Workaround: You can perform a manual reconfiguration reboot after the first cluster installation fails by issuing the following command:

```
/usr/bin/touch /reconfigure; /usr/sbin/shutdown -y -i6 -g0
```

Once the system is back up, you can run the install cluster job again.

QCCR1D: 93208

Description: Links to vendor documentation for Solaris patches that point to a local HTTP server do not work.

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: Vendor documentation URLs that point to a local HTTP server are not displayed correctly causing the URL to fail.

Workaround: Open the vendor documentation in a browser.

QCCR1D: 93494

Description: solpatch_import: with Patch Management=Read/None script returns "Authorization Denied" when importing patch, but the patch is actually imported to Library

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: Using the SAS Web Client, change the Patch Management permission to `Read` or `None` for a User Group. In the configuration file, specify `hpsa_user/pass as username/password>`.

When you attempt to import a patch, the following error is displayed:

```
141104-01: Authorization Denied.  Not able to import patch
```

However, login to SA Client with the username/password for the user group specified above and select **Library ➤ Patches ➤ Solaris ➤** <operating system>, the patch is shown as imported and displayed in the Library.

Workaround: None

QCCR1D: 93502

Description: Preview of a Solaris patch install fails with an "unknown reason" error when there is not enough disk space available on the target Solaris server.

Platform: Solaris

Subsystem: Solaris Patching

Symptoms: Previewing the installation of a Solaris patch fails and gives an error like the following:

```
The request to retrieve information from the Agent failed for an unknown
reason, please contact your HP Server Automation Administrator.Execution
error: Traceback (innermost last):
 File "./base/wayfuncs.py", line 136, in evaluator
 File "<string>", line 1194, in ?
 File "<string>", line 1185, in main
 File "<string>", line 393, in findTmpdir
OpswareError:
 args: ()
 been_cascaded: 0
 error_name: cogbot.packageDownloadInsufficientSpace
 faultCode: 101
 faultString: cogbot.packageDownloadInsufficientSpace
 hostname: m164.qa.opsware.com
 line: 393
 method: findTmpdir
 module: <string>
 params: {'space_needed': '119101L kb', 'paths': ['/var/opt/opsware/agent
 88000 kb']}
 request: UNKNOWN
 tb_chain: []
 timestamp: 20/Mar/2009 200121
 timeticks: 1237579281L
cogbot.packageDownloadInsufficientSpace
```

Workaround: Ensure the Solaris server has adequate disk space to install the patch.

QCCR1D: 93689

Description: SA 7.80 does not support installing Solaris patch clusters that require a password.

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: If you attempt to install a Solaris patch cluster that requires a password, the install job will fail with a message stating that SA 7.80 does not support Solaris patch clusters that require a password.

Workaround: Install the Solaris cluster manually on your managed servers. Once you install the cluster, SA will detect that the patches in the cluster have been installed on your managed servers.

QCCR1D: 94074

Description: User/Group objects can be added into Solaris patch policy, this should not be allowed.

Platform: Solaris

Subsystem: Solaris Patch Management

Symptom: If you select a User/Group object from the Server Browser and select **Add to Software Policy**, Solaris patch policies are also listed and you can select a Solaris patch policy and add it but this should not be allowed.

Workaround: Do not add User/Group objects to Solaris Patch Policies even if it appears to be allowed.

Patch Management for Windows

Bug ID: 132400 / QCCR1D: 43934

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

Platform: Windows

Subsystem: Patch Management for Windows

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

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

Bug ID: 132599 / QCCR1D: 44101 (see also 142923/54277)

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

Platform: Windows

Subsystem: Patch Management for Windows

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

Workaround: None

Bug ID: 132866 / QCCR1D: 44304

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

Platform: Windows

Subsystem: Patch Management for Windows

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

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

QCCR1D: 91441

Description: Various Windows patch management issues.

Platform: Windows

Subsystem: Patch Management for Windows

Symptom1: Microsoft Patch KB940767: You may find that Update Rollup Q940767 is on the list of patches recommended by the vendor for your Windows servers. This patch contains the IE7 installer. If you install this patch, the job result will be Completed with Warnings. The Job Details will show that patch Q940767 was not installed, and that a number of other patches were installed as a side effect. When you investigate the server, you will find that IE7 and several other components are installed. Because MBSA does not detect that Q940767 is installed, this patch will not appear on the list of patches installed, nor will it show on the list of patches recommended by the vendor. MBSA's failure to detect the presence of Q940767 will not affect the compliance status of your server

Workaround: None

Symptom 2: SA cannot uninstall Windows Rights Management Client Service Pack 2, KB917275.

Workaround: If you need to remove this Service Pack, you can use Add/Remove Programs on the server.

Symptom 3: There are no Service Packs available for Windows 2000 server that SA can uninstall; therefore, uninstalling Service Packs on Windows 2000 servers has not been tested.

Workaround: None

Symptom 4: Uninstalling Windows patches may cause problems on your server if you uninstall in the wrong order.

Workaround: For more information, please read the article “Removing Windows software updates in the wrong order may cause the operating system to stop functioning” at *http://support.microsoft.com/kb/823836*.

Symptom 5: Windows servers must be rebooted after installing and uninstalling Service Packs. You should not change the reboot flags on Service Pack patch browsers.

Workaround: None

Symptom 6: If you install a patch that was recommended by the vendor and then uninstall the patch, it may not reappear on the list of patches recommended by the vendor. When a patch is uninstalled from a Windows server, underlying `.dlls` and `.exes` may not be removed and MBSA may not detect that the patch is not installed.

Workaround: None

Symptom 7: If you use DET (CBT) to import patches, patch policies, software policies with attached patches, or server groups that have attached software or patch policies, the result may be unexpected if any of the following patches are imported from a pre-SA 7.80 Core:

- MS09-003 (KB959897) for Windows 2000
- MS09-004 (KB960082) for Windows Server 2003 or Windows Server 2003 x64
- .NET Framework 3.5 Service Pack 1 for Windows XP, Windows Server 2003, Windows Server 2003 x64, Windows Server 2008 or Windows Server 2008 x64

There are duplicates of these patches in the February MBSA patch database and SA 7.80 removes the duplicates. If you run a DET import that includes one of these patches, the patch placeholders (the patch binaries will not be available) can be deleted from your core. One way to identify these patches is to display the locale column and delete those patches that do not have any value for locale.

Workaround: None

Symptom 8: If the registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\TrustedPublisher Safer` exists, it can cause Windows patch compliance scans and patch install/uninstall and remediate jobs to fail.

Workaround: None

QCCR1D: 92308/92415

Description: When remediating Windows patch policies containing more than one Windows patch, it is possible for some patches to not install correctly because supersedence information is incorrectly considered. For example, this can happen in the case where patch A is superseded by patch B which is superseded by patch C. When remediating a policy that contains patch A and patch C, SA may install patch C first, then install patch A, which results in patch A failing to install because a superseding patch (i.e. patch C) is already installed.

Platform: All Windows platforms

Subsystem: Windows patching

Symptom: Remediate patch policy jobs may end with an error because a superseding patch is already installed.

Workaround: None

Patch Management for Unix

Bug ID: 138929 / QCCR1D: 50283

Description: Unclear error message when base fileset and update fileset does not uninstall successfully during Patch remediation.

Platform: AIX 5.3

Subsystem: SA Client - Patch Management for Unix

Symptom: If you attempt to use the Patch Remediate feature to uninstall the base fileset and update fileset on the AIX 5.3 operating system in one remediation job, the install base fileset and its update should both be uninstalled. In the particular case, when uninstallation of base fileset fails, the error message is not clear enough to indicate the reason, and the update fileset is not mentioned in the error messages.

Workaround: None

Bug ID: 139165 / QCCR1D: 50519

Description: APARs can be satisfied by both Update Filesets and Base Filesets.

Platform: AIX

Subsystem: SA Client - Patch Management for Unix

Symptom: If the LPP containing the Base Fileset that satisfies an APAR is uploaded with the Import Package dialog, SA does not recognize that the Base Fileset satisfies the APAR. When you view the APAR properties, you will see `Unknown AIX Fileset` for the Base Fileset that was just uploaded.

Workaround: Upload the LPP containing the Base Fileset using the OCLI with the `-o` option. Verify that the `-C` customer option specifies Customer Independent.

QCCR1D: 93840

Description: Installing AIX APARs may give a message indicating some file sets cannot be found.

Platform: AIX

Subsystem: SA Client - Patch Management for Unix

Symptom: When attempting to install an APAR, some of its file sets may not be installed with a message indicating the file sets cannot be found. When attempting to view the file sets the APAR contains, some file sets will show up as missing or unknown.

Workaround: If you are certain the missing file sets have been imported to SA, this may be due to an issue with how APARs are mapped to file sets. To work around the issue, log in to any core running the Software Repository and run the following command:

```
/opt/opsware/mm_wordbot/util/migrate_aix_metadata -m
```

PowerShell

Bug ID: 154417 / QCCR1D: 65771 (see also 155866/67220, 156132/67486)

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

Platform: Windows

Subsystem: PowerShell

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

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

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

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

{ write-host "Found file"}

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

Bug ID: 158784 / QCCR1D: 70138

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

Platform: Windows

Subsystem: PowerShell

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

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

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

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

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

Workaround: None.

Bug ID: 153788 / QCCR1D: 65142

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

Platform: Windows

Subsystem: PowerShell

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

Workaround: None.

Bug ID: 159364 / QCCR1D: 70718

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

Platform: Windows

Subsystem: PowerShell

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

Workaround: Install PowerShell on the managed server.

Bug ID: 158487 / QCCR1D: 69841

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

Platform: Windows

Subsystem: PowerShell

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

Workaround:

1. Create a batch file with the following command:

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

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

QCCR1D: 65105

Description: Unable to run a Windows PowerShell script from the Global shell.

Platform: Windows

Subsystem: PowerShell

Symptom: When you run a PowerShell script from the Global shell on any Windows system, the script does not run. Instead, Windows opens the script in the Notepad application.

Workaround: Run the PowerShell script from the SA Client. For more information on the PowerShell, see the *SA Platform Developer's Guide*. For more information on the Global Shell, see the *SA User's Guide: Server Automation*.

QCCR1D: 87591

Description: PowerShell appears not to install on non-English locale managed servers.

Platform: Windows

Subsystem: PowerShell

Symptom: When installing PowerShell using the SA Client on non-English locale servers, the installation appears to fail with the following error:

```
Cause: com.opsware.common.LegacyException
Exception Message: Summary: An error occurred while installing or removing
this package.
Detail: An error occurred while installing or removing this package. The
package may not be applicable for the selected server.
```

However, PowerShell does in fact install correctly.

Workaround: After the PowerShell installation appears to finish unsuccessfully, log into the server and run PowerShell.exe. Then run this command:

```
$ Add-PSSnapin OpswareSasPs
```

This will load the SA PowerShell snapin. PowerShell should function normally thereafter.

SA API

QCCR1D: 60101

Description: This is not a defect, but rather a change to the SA API. The UnitService.update() method API signature has been changed in a way that is incompatible with the previous method signature. The new signature throws a new exception, InvalidPlatformAssignmentException.

Platform: All

Subsystem: API

Symptom: If you are using this method, your custom code may not work properly.

Workaround: If you are using this method, you must examine your code and rewrite the calls to conform to the new signature. For more information, see the SA Twister API documentation and the *SA Platform Developer's Guide*.

SA Client

Bug ID: 133253 / QCCR1D: 44607

Description: Actions available for the search results are not accurate if multiple windows are open in the SA Client.

Subsystem: SA Client - Search

Platform: Independent

Symptom: After performing a search in the SA Client, If you open multiple windows and select objects in more than one window, then the actions available for the search results from the Action menu for the selected objects may in incorrect in the other windows.

Workaround: To display the exact options in the Action menu for the search results, reselect the objects in the active window and then select **Actions** from **the** File menu.

Or

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

Bug ID: 138334 / QCCR1D: 49688

Description: Job Type drop-down list for both Job Logs and Recurring Schedules may not display correct available jobs if a user's permissions change while the SA Client is open.

Platform: Independent

Subsystem: SA Client - Jobs and Sessions

Symptom: Depending on when a user's granted permissions change, for example, while the user is logged in to the SA Client, the Job Logs and Recurring Schedules Job Types drop-down list may not display the available job types accurately for that user. For example, if a user has permission to view all job type when the user starts the SA Client, but during the session has a change in permissions that allow the user to not view certain job types, the Job Type drop-down list will still display all jobs as being available to view by the user.

Workaround: Close and restart to the SA Client, or open a new window in the SA Client and check the Job Types drop-down list again.

Bug ID: 144363 / QCCR1D: 55717

Description: Duplicating a device group from a device group without any rules, results in duplicate device group showing to contain servers.

Subsystem: SA Client - Device Groups

Platform: Independent

Symptom: In the SA Client you can duplicate a dynamic group which contains no rules and the resulting duplicate device group shows up in the device group list. In the navigation pane, when you select the duplicate device group, the members of the device group are shown in the Content pane.

Workaround: Create a rule for each dynamic device group or convert the dynamic device group to a static device group.

Bug ID: 159906 / QCCR1D: 71260

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

Platform: Independent

Subsystem: SA Client - Oracle

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

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

```
<datestamp>
Errors in file /u01/app/oracle/admin/truth/udump/truth_ora_0000.trc:
ORA-00600: internal error code, arguments: [kkslgbv0], [], [], [], [], [],
[],[]
```

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

Workaround: If you have previously worked around this problem by setting the Oracle parameter `CURSOR_SHARING=EXACT`, you should upgrade your SA Oracle instance to 10.2.0.4 or 11g and change this parameter back to the SA recommended default of `CURSOR_SHARING=SIMILAR`. This will improve the performance of the your SA Oracle database.

QCCR1D: ID: 81032

Description: Device Explorer Local Security Settings Server Module loading error for some objects on Windows 2000 SP4

Subsystem: Device Explorer/Local Security Settings Server Module

Symptom: When loading the Windows Security Settings Server Module in a server's Device Explorer for a Windows 2000 SP4 server, some of the objects retrievable return the following message: `Error retrieving value`.

For example, if you try to load Local Security Settings -> Security Options, some of the objects will not load, and return an error. This is due to the Windows Management Instrumentation (WMI) not being installed on the server.

Workaround: Make sure that the Windows 2000 SP4 server you are browsing has WMI installed.

QCCR1D: 90964

Description: Size Limit on SA Client Object URLs

Platform: Windows

Subsystem: SA Client

Symptom: When you drag and drop or copy and paste a URL from the SA client (by selecting one or more rows from any of the tables), it generates a URL which links back to the selected object in the client. These URLs can be long if many rows are selected and some windows clients have limits on the URL length. If the URL is too long, then the selected object referenced by the URL will not be launched.

Workaround: Use a service like tinyurl.com to shorten the URL.

QCCR1D: 93215

Description: Searching for Solaris patch clusters using Advanced search in the SA client sometimes returns deleted Solaris patch clusters.

Platform: All Solaris platforms

Subsystem: SA Client, Advanced search

Symptom: Delete an existing Solaris Patch cluster and run a search for Solaris patch clusters. The search returns the Solaris patch cluster that was deleted. Search should return only the Solaris clusters that were not deleted.

Workaround: None

QCCR1D: 93876

Description: Performing an advanced search for patches using a filter of "Last Modified By" returns patches that were not last modified by the specified user.

Platform: Windows and Solaris

Subsystem: Advanced search in the SA Client

Symptom: Performing an advanced search for patches using a filter of "Last Modified By" returns patches that were not last modified by the specified user.

Workarounds: Search using other criteria.

SA Installer

Bug ID: 149334 / QCCR1D: 60688

Description: The -a option does not accept uploads if it is in the same action file as other components.

Subsystem: SA Installer

Platform: Independent

Symptom: You tried to install a core with the following action file:

```
[root@ruby1 root]# cat action_file1
%components
truth
owc
word
spin
way
osprov_buildscripts
osprov_boot
osprov_media
gateway_ha
shell
word_uploads
osprov_stage2s
oracle_sas
```

Since the SA Installer is run from the primary distro, the content upload failed. The SA Installer prompted you for the upload distro, but did not accept the valid entry.

Workaround: Remove `word_uploads` and `osprov_stage2s` from the primary action file and then create a new action file that is used by the SA Installer when it is run from the upload distro.

SA/SAR Reports

Bug ID: 133350 / QCCR1D: 44704

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

Platform: Independent

Subsystem: SA Client - Reports

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

Workaround: Click the **Show all <*nn*> Servers** link to view the correct multi-byte characters.

Bug ID: 133351 / QCCR1D: 44705

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

Platform: Independent

Subsystem: SA Client - Reports

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

Workaround: Click the **Show all <*nn*> Servers** link to view the correct multi-byte characters.

Bug ID: 133652 / QCCR1D: 45006

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

Platform: Independent

Subsystem: SA Client - Reports

Symptom: Logon to the NGUI. Run Reports > Servers by Customer. Select the Equals operator. Select a customer that has multi-byte character(s) in the name. Click Run. The characters ??? are displayed in the Report Description instead of the correct multibyte character. Multibyte characters are displayed correctly in the report output, but incorrectly in the report header.

Workaround: None. This occurs due to a bug in the BIRT report engine.

Bug ID: 136029 / QCCR1D: 47383

Description: The Action menu is disabled in Reports.

Platform: Independent

Subsystem: SA Client - Reports

Symptom: When the Reports feature is selected in the navigation tree, the Action menu is disabled.

Workaround: Use the context-sensitive (right-click) menu.

Bug ID: 143410 / QCCR1D: 54764

Description: The SA Client "Servers by Customer" report fails to return complete results on desktops with less than 1 GB MB RAM and when the number of servers is greater than 1000.

Platform: Windows

Subsystem: SA Client - Reports

Symptom: In the SA Client, if you run the following report, Server Reports ➤ Servers by Customer, the report takes a long time to complete on machines with less 512 MB RAM and

when you attempt to run the report on more than 4000 servers. Moreover, the report will not export to CSV — only the first few hundred records will be exported.

Workaround: To run this report, it is recommended that the system from which you are running the report has at least 1GB of memory, and you limit the number of servers to 1000.

If the report completes, export the report to HTML. Then, open the report in a Web browser, select all and then copy. Then, open Excel, select the whole sheet then perform an Edit ➤ Paste.

Bug ID: 147624 / QCCR1D: 58978

Description: In the Reports feature, the Remote Terminal connects to the wrong server.

Subsystem: SA Client - Reports

Platform: Independent

Symptom: Run the Server by Customer Report. Select a Unix server in the report and launch a Remote Terminal to it. Exit out of the Remote Terminal and sort the list by selecting "customer". Select a different server, right-click, and then select a Remote Terminal. This action will take you to the previously-selected (wrong) server.

Workaround: You must first left-click to select a row and then right-click so that an action in the **Option** menu correctly applies to the selected object.

SAR Client/SAR Server

QCCR1D: 89242

Description: For SAR 7.80 installs on an SA core with multiple Slice Component bundles, enable_omdb_client.sh script must be run on each slice in the core to enable the SAR feature.

Platform: Independent

Subsystem: SAR Configuration

Symptom: If you are installing the SAR 7.80 core services server in a SA 7.80 core with multiple Slice Component bundles, you need to run the enable_omdb_client.sh script on each host on which you installed the SA Web Services Data Access Engine (twist) (part of the Slice Component bundle) or SAR will not report for data for that host.

Workaround: If you are enabling SAR 7.80 on an SA 7.80 deployment with no slices, you need to run the enable_omdb_client.sh script on the server where you installed in the Web Services Data Access Engine (twist). However, if you have installed your SA Core with

multiple Slice Component bundles on different hosts (therefore, multiple Web Services Data Access Engines on different hosts), you must run the script on each Slice Component bundle host in your mesh.

QCCR1D: 91103

Description: The SAR 7.80 patch cannot be installed on a SAR core services server that is installed on the same server as SA.

Platform: Independent

Subsystem: SAR Installation

Symptom: In SAR and SA 7.80 release, installing a SAR core on the same server as an SA core is not supported.

Workaround: Install the SAR 7.80 core services server on a separate server from the SA core.

QCCR1D: 93972

Description: After a Search for User is performed, the results may presented incorrectly, with duplicate columns and incorrect data mapping.

Platform: Independent

Subsystem: SAR Client

Symptom: If you perform a search for SA Users in the SAR Client, the results may be displayed with improper formatting. For example, the User name column is duplicated; instead of user name data the <first name> is displayed; instead of account status there is <last name> displayed; and so on.

Workaround: If the client Search results pane shows duplicated columns, or data in incorrectly headed columns, change the Configuration Item (CI) type selected in the Advanced Search pane, then change CI type back to the original one. This should reset display column selection to the default for the CI and resolve the incorrectly-displayed data.

QCCR1D: 93979

Description: Incorrect reference to internationalization support for SAR 7.80 in online documentation

Platform: Independent

Subsystem: SAR Client Launcher

Symptom: In the online help and in the SAR User's Guide PDF, section titled “SAR Client Launcher Advanced Options,” there is an incorrect reference to support for localized systems that states: “Choose a locale to match the localized version of the SAR Client, either Japanese (ja), Korean (ko), or English (en). English is the default.” This is incorrect. SAR Client does not support internationalization.

Workaround: None.

However, SAR 7.8 does support the mining and display of multibyte characters; for example, the SAR Client can display Korean words used for naming saved searches, SA user details, security boundary names, and so on, independent of the locale selection and user profile locale settings. In order to display multibyte characters, supplemental language support (for Asian languages) must be installed on the computer where the SAR client is running.

QCCR1D: 94113

Description: After upgrading SA and SAR to 7.8, search results do not display in the SAR Client.

Platform: Independent

Subsystem: SAR Client

Symptom: After an upgrade to SA and SAR 7.80, the Oracle User account CMDB_REPORTER on the SAR box becomes locked. After unlocking the CMDB_REPORTER account, the SAR core and searches seem to function as expected.

This may occur when scheduled SAR tasks belonging to multiple users are running during the SAR upgrade.

Workaround: Check the CMDB_REPORTER user account after upgrading and unlock the user account.

QCCR1D: 91422

Description: When generating reports on storage data, the SQL query will output nearly a hundred WARN messages with SQL Exceptions.

Platform: Independent

Subsystem: SAR Client

Symptom: In some cases, when you run a report that is based upon storage data, the SQL query will generate many WARN messages with SQL Exceptions, all of which are written to the server.log file.

Workaround: These messages are harmless and can be ignored. The deployer service is attempting to create foreign key constraints on data fields where they are not required. This issue will be addressed with a fix in a future release.

SAS Web Client

Bug ID: 136366 / QCCR1D: 47720

Description: `TimedOutException` occurs when deleting a dynamic server group containing many servers.

Subsystem: SAS Web Client

Platform: Independent

Symptom: In the SA Web Client, when you delete a dynamic server group containing many servers, the following exception occurs:

```
Error Summary
Name:   Standard 500 Error
Description:    500 Internal Server Error
More Details...
Hide Details
Message Text:   Transaction Rolledback.; nested exception is:
weblogic.transaction.internal.TimedOutException: Transaction timed out after
243 seconds
```

In spite of the exception, the dynamic server groups are deleted successfully.

Workaround: None

Bug ID: 148022 / QCCR1D: 59376

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

Platform: Independent

Subsystem: SAS Web Client - Environment

Symptom: In HP Server Automation 5.x and earlier, when a managed server first registers with a core, a customer can be associated with the server if the server is within the IP range for that customer. However, this automatic association does not work if the managed server contacts the core through an SA Gateway, which is the case for HP Server Automation 5.x and later. The SA Policy Setter's Guide mistakenly tells the reader that associating servers with customers through the use of IP ranges still works.

For more information on this bug, see the description for bug ID 132880.

Workaround: Assign the customer to the managed server after deployment.

Bug ID: 154691 / QCCR1D: 66045

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

Platform: Independent

Subsystem: SAS Web Client

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

Workaround: None

QCCR1D: 89156

Description: NGUI value set editor always uses default order, disregarding the UAPI specified order.

Platform: Independent

Subsystem: Independent

Symptoms: Device group precedence is being ignored by the NGUI. No matter what order is specified via the UAPI, the NGUI continues to use default order.

Workaround: None

QCCR1D: 82947/89329

Description: Java Exceptions and SAS Web Client display issues occur when the Windows Desktop theme is changed.

Platform: Windows

Subsystem: SAS Web Client

Symptom: After changing the Windows Desktop theme, for example from blue to silver, the SAS Web Client displays exceptions, has display problems, and must be restarted.

Workaround: None. If exceptions and display problems occur, you must restart the client.

Script Execution

Bug ID: 155135 / QCCR1D: 66489

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

Platform: Independent

Subsystem: Script Execution

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

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

then the following null pointer exception is thrown:

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

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

Bug ID: 157422 / QCCR1D: 68776

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

Platform: Independent

Subsystem: Script Execution

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

1. In the script window, select a Version History from the navigation pane
2. From the Content pane, select a script

3 From the File menu select Set as Current Version

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

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

Workaround: None.

Bug ID: 159213 / QCCR1D: 70567

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

Platform: Independent

Subsystem: Script Execution

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

Manage Server Scripts: Read

Folder Permission: Execute objects in Folder.

Workaround: None.

Defect QCCR1D: 71383

Description: Importing and then exporting a Unicode UTF8 script can insert spurious characters into the script.

Platform: Any

Subsystem: Importing a script/SA Client

Symptom: If you import a script that uses Unicode (UTF8) encoding and your computer's regional language settings are set to English, and then you export the script and attempt to execute it, you may encounter errors because Unicode (UTF8) encoding may add a "." or other special character at the beginning of the script.

Workaround: Open the file and edit the script to remove the extraneous characters. For more information, see "Script Execution" in the *SA User Guide: Application Automation*.

Server Agent

Bug ID: 129735 / QCCR1D: 41801

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

Subsystem: SA Client, Agent Deployment

Platform: Independent

Symptom: When you scan a server that is already managed by SA, the ODAD feature cannot determine which managed server ID it corresponds to and, by default, opens the unmanaged server window.

Workaround: None

Software Discovery

QCCR1D: 83281

Description: Software Discovery reports show empty results when the device group selected is one of the default parent groups.

Subsystem: Software Discovery

Platform: Independent

Symptom: When there are servers under a default parent group (such as **All windows Servers**), the servers are displayed. If there are no servers under the parent group but there are servers in a subgroup, they will be displayed in the subgroup but not in the parent group.

Workaround: None, by design

Software Management

Bug ID: 133443 / QCCR1D: 44797

Description: Bulk package upload can cause the `Package Type Not Defined in Truth` error.

Subsystem: SA Client - Software Management

Platform: Independent

Symptom: Import media uploads packages to the Software Repository. The Software Repository connects to the Data Access Engine to retrieve information specific to the package type being uploaded. Even though all packages uploaded during this step are of the same type, the call to the Data Access Engine will occasionally produce the following error: `Error uploading package. SUNWceax: Package Type Not Defined in Truth`.

Workaround: None.

Bug ID: 138400 / QCCR1D: 49754

Description: Software is not uninstalled after a migrated software policy is detached and remediated from a server

Platform: Independent

Subsystem: Software Management - Content Migration

Symptom: If you detach a migrated software policy from a server and remediate, the packages are not removed from the server.

Workaround: You can install software by using a migrated software policy in the SA Client but you cannot uninstall software until you have completed the migration. You must complete migration as soon as possible and do not remediate servers or detach software policies unless you have completed migration.

Bug ID: 143642 / QCCR1D: 54996

Description: Remediating an RPM package to a server in one core immediately after importing the package in another core in a multimaster mesh fails with metadata missing error.

Platform: Independent

Subsystem: SA Client - Software Management

Symptom: In a multimaster mesh, after importing an RPM package in one core, if you try to install the package in another core immediately, then the remediation fails with metadata missing error.

Workaround: If you receive this error immediately after importing an RPM in one core and then attempting to install the RPM on a server in another core, wait several minutes, then retry the operation.

Bug ID: 143751 / QCCR1D: 55105

Description: Uninstall fails for `zope` packages on Suse Linux Enterprise Server 10.

Subsystem: SA Client - Software Management - RPM Deployment

Platform: Linux

Symptom: In the SA Client, when you try to uninstall a `zope` package on Suse Linux Enterprise Server 10 server by remediating the server with a software policy containing `zope` package, the remediate process fails with the following error:

```
ImportError: /opt/zope/lib/python/ZODB/cPersistence.so: wrong ELF class:
ELFCLASS32
..failed
error: %preun(zope-2.7.8-15.i586) scriptlet failed, exit status
Software uninstall failed with an exit code of 255
```

Workaround: To uninstall a `zope` package on a Suse Linux Enterprise Server 10 server, add `--noscripts` to the uninstall properties of the `zope` package in the Package Properties window before remediating the server.

Bug ID: 144220 / QCCR1D: 55574

Description: Performance issues when remediating a policy containing a large number of RPMs.

Subsystem: SA Client - Software Management - RPM Deployment

Platform: Linux

Symptom: When remediating a policy which contains a large number of RPMs, the SA Client does not appear to be performing any action.

Installing RPMs contains consists of three phases.

Phase 1: Resolve dependencies for the RPMs contained in the policy.

Phase 2: Download the RPMs resulting from phase 1.

Phase 3: Install the RPMs.

Phase 1 corresponds to the “Preview” step of remediating a policy.

Even if the “Preview” button is not clicked, this phase must still be performed. While this phase is occurring, the SA Client does not provide any feedback. If many RPMs (more than one hundred) are involved, this step can take up to 45 minutes to complete. Although nothing appears to be happening in the SA Client, in reality, SA is performing the steps needed to resolve dependencies. Because this phase involves many transactions between the managed server and the SAS core, the operation is not instantaneous.

Workaround: None.

Bug ID: 146298 / QCCR1D: 57652

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

Platform: Independent

Subsystem: Software Management

Symptom: As an Administrator user, editing the /Opsware/Tools folder in the Library in the SA Client may result in the following:

Inability to install RPMs
Inability to remove RPMs
Inability to upgrade RPMs

Workaround: Do not edit the /Opsware/Tools folder in the Library

Bug ID: 148745 / QCCR1D: 60099

Description: Pre or Post install scripts specified for HPUX Products are not executed on the managed server during remediation.

Platform: Independent

Subsystem: Software Management

Symptom: For HPUX products, if you specify any pre or post install scripts on the Package window and then add the HPUX package to a software policy and remediate the server, then the HPUX packages are installed successfully, but the pre or post install scripts are not executed on the server.

Workaround: None.

Bug ID: 148797 / QCCR1D: 60151

Description: Compliance status of a managed server does not get updated after remediation, if the server is in the destination core in a multimaster mesh.

Platform: Independent

Subsystem: Software Management

Symptom: In a multimaster mesh, if the managed server is in a remote core, in other words, the SA Client is connected to a different core, then when the managed server is remediated with a software policy, the compliance status may not reflect the correct result. But the software resources specified in the software policy are installed on the managed server.

Workaround: None

QCCR1D: 90967

Description: Attaching a Software Policy to a new OS sequence does not limit sequences to the platform selected in the OS Profile.

Platform: Independent

Subsystem: Software Management

Symptom:

1. Select **New Sequence**
2. Fill in the Name, OS Profile and customer
3. Go to the Software Policy task and select **Add Policy**:
   - **Expected Behavior**: Only Software Policies of the platform selected by the OS Profile should be displayed
   - **Actual Behavior**: All Software Policies are displayed

Workaround: Either find the Software Policy by browsing the folders or Save, close and then reopen the OS Sequence.

Bug ID: 93428

Description: Install Software fails with `LegacyException` on SunOS 5.10 Local Zone.

Platform: Solaris

Subsystem: Software Management

Symptom: When a Solaris Local Zone is configured with a sparse root (shared `/sbin`, `/lib` and `/usr`), an error occurs when installing/uninstalling packages. According to Sun documentation, `patchadd` will fail when patching an area shared with the Global Zone.

Workaround: None

Software Repository

Bug ID: 149059 /QCCR1D: 60413

Description: If the Software Repository server is marked unreachable when you try to upload the SA content component, the upload process fails.

Subsystem: Software Repository

Platform: Independent

Symptom: You tried to upload the SA content component when the Software Repository server was marked unreachable. The upload failed with a `wordbot.accessDenied` error.

Workaround: Run the server communications test to verify whether the Software Repository server is marked unreachable.

Virtualization

QCCR1D: 89739

Description: Creating or Modifying a VM with non-ASCII characters in the name/description causes invalid display of the name/description.

Platform: VMWare

Subsystem: Virtualization

Symptoms: Creating a VMWare Virtual Machine (VM) on a Hypervisor with a name that contains non-ASCII characters results in the name/description displaying ? rather than the non-ASCII characters. This occurs when the Slice Component bundle host's locale settings are not configured for UTF-8 encoding. Specifically, the error occurs on SUSE Linux Enterprise Server 10 hosts for which the locale-specific system settings are not in effect when the SA components start up as a service during system initialization.

Workaround:

1. Set the following locale-specific environments in the shell environment:

   ```
   LANG=en_US.UTF-8
   LC_ALL=en_US.UTF-8
   export LANG
   export LC_ALL
   ```

2. Restart the hub:

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

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

Symptoms: 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: 92426

Description: A Local Zone's Installed Patches list does not display patches that were installed using a Global Zone Patch Policy remediation.

Platform: Solaris Zones

Subsystem: Virtualization

Symptoms: Remediate a patch policy that contains patches applicable to both the Local and Global Zones, attach the patch policy only to the global zone. The patches should be installed on both the Local and Global Zones, however, the Server Browser **Installed Patches** list shows the above patches as installed only on Global Zone.

Workaround: None

QCCR1D: 93123

Description: If you attempt to create a virtual machine (VM) and have an old job window open at the same time, the Create VM job fails with an error stating that the VM name already exists.

If you attempt to run two or more Create VM jobs at the same time, SA incorrectly attempts to create multiple instances of the VM with the same name.

If you attempt to run two or more Modify VM jobs at the same time, SA incorrectly modifies one VM twice.

Platform: VMWare

Subsystem: Virtualization

Symptoms: The Create Virtual Machine job displays an error dialog stating: “Use a different name. Virtual server already exists with this name.” In the modify VM case, one VM gets modified twice.

Workaround: When you create a virtual machine, close all other old job windows and only create one virtual machine at a time. When you modify a virtual machine, close all other old job windows and only modify one virtual machine at a time.

QCCR1D: 93703

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

Platform: VMWare

Subsystem: Virtualization

Symptoms: SA creates multiple VMs until the hypervisor runs out of resources.

Workaround: When creating a VM and at the same time attempting to provision an OS, you must configure only one network interface for the VM to use. You must also select the “Connect at Power On” option.

QCCR1D: 94207

Description: ESX feature **Open Console** does not work.

Platform: VMWare ESX

Subsystem: Virtualization

Symptoms: When you right click a VMWare ESX VM, and select **Open Console**, the login dialogue is displayed, but the message `Web service is unavailable` is also displayed.

Workaround: Right click the Hypervisor for the VM and select the option **Open Web Access** from which you can navigate to the VM console.

Windows Security Settings

QCCR1D: 70593

Description: The following security settings may be reported or set incorrectly for Windows XP servers:

- Password Policy:
  - Password must meet complexity requirements
  - Store password using reversible encryption for all users in the domain
- Security Options:
  - Accounts: Administrator account status
  - Accounts: Guest account status
  - Accounts: Rename administrator account
  - Accounts: Rename guest account
  - Network access: Allow anonymous SID/Name translation

Platform: Windows XP

Symptoms: When you view security settings for a Windows XP server, or set up a snapshot or an audit for a Windows XP server, some security settings may be incorrect.

Remediating differences in audit results on a Windows XP server may also fail because of incorrect security settings.

Workaround: Install Windows hotfix 897372 or Windows XP Service Pack 3. For more information, see http://support.microsoft.com/kb/897327.

WS v2.2 DSE Service Tests

QCCR1D: 63360

Description: Webservices version 2.2 DSE tests are not functional.

Platform: Independent

Subsystem: Webservices version 2.2 DSE Service Tests

Symptoms: Webservices version 2.2 is not supported on fresh SA 7.80 installs. The Webservices version 2.2 tests can be run only on migrated SA 7.80 Cores.

Workaround: The integration user has no folder and therefore does not have access to private scripts unless a folder is specifically created for that account. You can:

- Create a folder for the integration user.
- Invoke a script API with a named user that already has a folder.

4 What's Fixed in SA 7.80

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 security reasons, SSL v2 hanshaking should be removed from the SA Agent. SSLv3 is supported.

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: 71989

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

Platform: Linux

Subsystem: Audit and Remediation

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: 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: 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

QCCR1D: 92144

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

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) can't be stopped properly because it can't be unmounted and the host must be rebooted before the OGFS can be started again.

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 permission which reference that object should also be removed. When the 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 `ISMRUNTIMEDIR` 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 (10.2.0.2) 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 10.2.0.2 database.

Resolution: Fixed

OS Provisioning

QCCR1D: 88820

Description: Samba version must be upgraded due to security issues 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 security problems and should be upgraded to a secure release.

Resolution: Fixed

Patch Management

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

Security

QCCR1D: 83898

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

Platform: Independent

Subsystem: Security - SSL

Symptom: A security 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

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

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: Fixed. 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

5 Documentation Errata

This chapter contains additional information to be added to the SA product manuals.

SA Administration Guide

The following should be added to the *SA Administration Guide*.

Chapter 6: SA Maintenance

In the section “Starting an SA Core Component”, subsection “Details: Component Start Order”, the start order list should read (this list assumes that Oracle for the Model Repository is already up-and-running):

- `verify_ports`: Verifies required ports are available
- `opswgw-mgw`: The Core Management Gateway
- `opswgw-cgws`: The Core Gateway
- `vaultdaemon`: The Model Repository Multimaster Component
- `dhcpd`: Required for OS Provisioning
- `spin`: The Data Access Engine
- `mm_wordbot`: Required for the Software Repository
- `waybot`: Required for the SA Command Engine
- `smb`: Required for OS Provisioning
- `twist`: The Web Services Data Access Engine
- `buildmgr`: Required for OS Provisioning
- `opswgw-agws`: The Agent Gateway
- `hub`: Required for the SA Global File System
- `sshd`: Required for the SA Global File System
- `apxproxy`: Required for the SA Global File System
- `spoke`: Required for the SA Global File System
- `agentcache`: Required for the SA Global File System
- `occ.server`: Required for the SAS Web Client
- `httpsProxy`: Required for the SAS Web Client
- `opsware-agent`: The SA Server Agent

Chapter 2: SA Core and Component Security

In Chapter 2, “SA Core and Component Security”, subsection “Core Certification”, the following should be added:

In the section, “Recertfying SA Cores”, Step 3, add the note:

The entry, `agent_recert.using_cdr` must set to 1 (true) if there are any Satellites in the mesh.

SA Planning and Installation Guide

Multimaster Installation, Phase 4

Restart the First Core Components

In this section, you are instructed on page 152 to restart the components in this order:

1. Data Access Engines (`spin`)
2. Web Services Data Access Engine (`twist`)
3. Model Repository Multimaster Component (`vaultdaemon`)

The correct order is:

1. Data Access Engines (`spin`)
2. Model Repository Multimaster Component (`vaultdaemon`)
3. Web Services Data Access Engine (`twist`)

Linux Package Requirements

Table 14: Required Packages For Linux AS3 32-bit x_86 (page 50) lists the package `libstdc++-devel` as required for Oracle support. This package *is not* required for Linux AS3 32-bit x_86, however *it is* required for Linux AS4 x86_64.

SA Policy Setter's Guide

The following sections are to be added to the *SA Policy Setter's Guide*.

Importing AIX Packages

In the chapter *Software Management Setup*, in the section “Importing a Package”:

The AIX package import tool makes it easy to import AIX packages (`*.bff` files) into SA. In addition, the tool may optionally create a policy from the imported packages. This simplifies the process of importing a collection of packages which comprise an AIX fix pack (that is, technology level or service pack).

Location

```
/opt/opsware/mm_wordbot/util/import_aix_packages
```

Usage

```
import_aix_packages [options]
```

All `*.bff` packages in the current working directory are copied to the SA library.

```
import_aix_packages [options] <source-directory>
```

All `*.bff` packages in the specified directory are copied to the SA library.

```
import_aix_packages [options] <*.bff>
```

The explicitly specified packages are copied to the SA library.

```
import_aix_packages -h
```

Show additional options.

Packages already in the SA library will not be copied unless you specify the `--force` option.

The operating system version of the packages will be determined automatically as long as a `bos.*` package is in the source list. Otherwise you must provide the AIX OS version using the `--os` option.

When importing packages comprising a *fix pack,* use the `-p <policy_path>` option to create an SA software policy containing the imported packages. `<policy_path>` specifies the location and name of the policy to create. For example

```
-p /AIX Fix Packs/ 5.3/5300-07-04-0812
```

OS Provisioning Hardware Support

In Chapter 3: *Operating System Provisioning Setup*, in the section "Hardware Support in OS Provisioning", subsection, "Adding Hardware Support to a Linux or VMware ESX Build Image", the paragraph:

The Linux Build Images are located on the OS Build Manager host in the following directories:

```
/opt/hp/buildscripts/linux/bi-<version>
```

Where `<version>` is the version of Linux.

should read:

The Linux Boot Images are located on the OS Boot Server host in the following directories:

Red Hat Linux 3 and 4:

```
/opt/opsware/boot/kickstart/rhel*/RedHat/base
```

Red Hat Linux 5:

```
/opt/opsware/boot/kickstart/rhel*/images/
```

There are two versions of each boot image. For example, the `rhel30` directory contains the Red Hat Enterprise Linux AS 3 boot image for x86 32- and 64-bit architectures, and the `rhel3ia` directory contains the boot images for Itanium architecture.

The Linux Build Images are located inside the OS installation media. The media is found in the media server.

Windows Server 2008 Provisioning

Sample Response File for Windows Server 2008

The following sample response file shows typical valid responses for a Windows Server 2008 installation in XML format. This sample response file contains the required settings for Windows Server 2008 provisioning with OS Provisioning.

The sample response file below will not work “as is”. You must edit it for your particular setup. You should refer to Microsoft's documentation for unattended file authoring (*Windows Automated Installation Kit (WAIK) User's Guide for Windows Vista*).

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
            <SetupUILanguage>
                <UILanguage>en-US</UILanguage>
            </SetupUILanguage>
            <InputLocale>en-US</InputLocale>
            <SystemLocale>en-US</SystemLocale>
            <UILanguage>en-US</UILanguage>
            <UILanguageFallback>en-US</UILanguageFallback>
            <UserLocale>en-US</UserLocale>
        </component>
        <component name="Microsoft-Windows-Setup" processorArchitecture="x86"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DiskConfiguration>
                <Disk wcm:action="add">
                    <CreatePartitions>
                        <CreatePartition wcm:action="add">
                            <Extend>true</Extend>
                            <Order>1</Order>
                            <Type>Primary</Type>
                        </CreatePartition>
                    </CreatePartitions>
                    <ModifyPartitions>
                        <ModifyPartition wcm:action="add">
                            <Active>true</Active>
                            <Format>NTFS</Format>
```

```
                            <Label>WinSrv08</Label>
                            <Letter>C</Letter>
                            <Order>1</Order>
                            <PartitionID>1</PartitionID>
                        </ModifyPartition>
                    </ModifyPartitions>
                    <DiskID>0</DiskID>
                    <WillWipeDisk>true</WillWipeDisk>
                </Disk>
            </DiskConfiguration>
            <ImageInstall>
                <OSImage>
                    <InstallFrom>
                        <MetaData wcm:action="add">
                            <Key>/IMAGE/Name</Key>
                           <Value>Windows Longhorn SERVERSTANDARDCORE</Value>
                        </MetaData>
                    </InstallFrom>
                    <InstallTo>
                        <DiskID>0</DiskID>
                        <PartitionID>1</PartitionID>
                    </InstallTo>
                    <WillShowUI>OnError</WillShowUI>
                </OSImage>
            </ImageInstall>
            <UserData>
                <ProductKey>
                    <WillShowUI>OnError</WillShowUI>
                    <Key>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</Key>
                </ProductKey>
                <AcceptEula>true</AcceptEula>
            </UserData>
        </component>
    </settings>
    <settings pass="generalize">
        <component name="Microsoft-Windows-PnpSysprep"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
            <PersistAllDeviceInstalls>true</PersistAllDeviceInstalls>
        </component>
    </settings>
    <settings pass="specialize">
        <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
            <OEMInformation>
                <HelpCustomized>false</HelpCustomized>
                <Manufacturer>HP</Manufacturer>
                <SupportHours>24x7</SupportHours>
                <SupportPhone>976-HELP</SupportPhone>
                <SupportURL>www.help.com</SupportURL>
```

```
            </OEMInformation>
        </component>
    </settings>
    <settings pass="oobeSystem">
        <component name="Microsoft-Windows-Deployment"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
            <Reseal>
                <Mode>Audit</Mode>
            </Reseal>
        </component>
    </settings>
    <cpi:offlineImage cpi:source="catalog:c:/documents and settings/
administrator/desktop/windows media/catalog files/x86/install_windows
longhorn serverstandardcore.clg" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

SA User Guide: Application Automation

In Chapter 9: *Operating System Provisioning*, the following section is to be added to the section, “Hardware Preparation”:

Booting an Itanium Server Using Elilo Boot

OS Provisioning supports booting a bare metal Itanium server using the Elilo preinstallation environment.

To boot a bare metal Itanium server using Elilo preinstallation environment, perform the following steps:

1. Mount the new Itanium server in a rack and connect it to the SA build network.
2. Configure the server to boot using Elilo.

   See the hardware vendor’s documentation on how to prepare a server to boot using Elilo
3. Power on the server and select the option to boot the server with Elilo.

   The SA menu appears and prompts you to select the type of OS Build Agent to install on the server.

   Choose an SA boot image by entering the appropriate text (linux, linux4, linux5, etc.) at the boot prompt:

   ```
   linux - Linux 3 Build Agent
   linux-txt - Linux 3 Build Agent for serial consoles.
   linux4 - Linux 4 Build Agent (default after 10 seconds)
   linux4-txt - Linux 4 Build Agent for serial consoles.
   linux5 - Linux 5 Build Agent
   linux5-txt - Linux 5 Build Agent for serial consoles
   ```

4 After the booting process finishes successfully, a message appears on the console indicating that the server is ready for OS provisioning. Since the OS Build Agent was installed, the server now appears in the Server Pool list in the SAS Web Client.

5 (Optional) Record the MAC address and/or the serial number of the server so that you can locate the server in the Server Pool list in the SAS Web Client or in the Unprovisioned Servers list in the SA Client.

You should verify that the newly racked server shows up in the SA Client Unprovisioned Servers or SAS Web Client Server Pool, and is ready to hand off for OS installation.

Virtual Machine and Hypervisor Must Be In the Same Facility

In the chapter "Virtual Server Management", the following should be added in the section "Creating a Virtual Machine".

When you create a virtual machine and provision the OS for the virtual machine, the virtual machine must be in the same facility as the hypervisor.

Installing Deferred-Activation Patches

In the chapter "Solaris Patching", the following is to be added to the section "Installing Solaris Patches".

On Solaris 10 only, installing Solaris Deferred-Activation Patches using the -t option to the patchadd command can cause problems. SA handles Deferred-Activation Patches by not using the -t option to patchadd when installing these types of patches.

Patch Management for Windows Prerequisites

In Chapter 6: Patch Management for Windows, the following bullet:

- For Windows Server 2008, the Add and Remove Programs dialogue must be closed when you run Windows patch management tasks.

should read:

- For all Windows Server versions, the Add and Remove Programs dialogue (Programs and Features in Windows Server 2008) must be closed when you run Windows patch management tasks.

Software Provisioning Action Script

The following is to be added to the chapter *Software Management*, to the section "Installing or Uninstalling Software".

When provisioning software, SA first creates a temporary download directory on the managed server. SA transfers the software to be installed to this directory, installs the software, then removes the temporary download directory.

SA provides a mechanism for running a script during software provisioning. One use for such a script is to integrate with a volume manager on the managed server. For an example, see AIX Volume Manager Integration Example on page 97.

Custom attributes on the managed server control the functionality as shown in Table 1:

Table 1 Software Provisioning Custom Attributes

Custom Attribute	Description
OPSWremediate_action_script	The name of a shared script (**SA Client ➤ Library ➤ By Type ➤ Scripts ➤ Unix**). For example, Remediate:AIX LVM Actions. You must provide the folder path when invoking the script: <path>/Remediate:AIX LVM Actions
OPSWremediate_action_script_args	Command-line arguments to provide to the script.
OPSWremediate_action_script_timeout	Time-out for the script in minutes. The default value is 1.
OPSWremediate_action_script_abort_on_error	Whether or not to stop the job if the script returns an error or times out. Legal values are “true” or “false” (case-insensitive), “yes” or “no” (case-insensitive) and “1” or “0”. The default is “true”. (This setting is effectively ignored if the “Attempt to continue running if an error occurs” checkbox which appears in the “Remediate Options” in the SA Client is checked.)

A software provisioning action script is run at four different points during the provisioning process. Several environment variables provide contextual information about the provisioning process to the script at the time it is run:

1 OPSWremediate_phase — The value of this environment variable is one of the following:

- pre-stage — This value indicates the script is to run just before the download operation.
- post-stage — This value indicates the script is to run just after the download operation has completed.
- pre-action — This value indicates the script is to run just before the software install operation.
- post-action — This value indicates the script is to run just after the software install operation has completed.

2 OPSWremediate_job_id — This value provides the ID of the current provisioning job.

3 OPSWremediate_space_required - This environment variable is set only during the pre-stage phase. Its value is the space in megabytes required to download the software.

4 OPSWremediate_download_dir — This environment variable is set only during the pre-stage phase. Its value is equivalent to the setting of the package_download_dir custom attribute on the managed server.

AIX Volume Manager Integration Example

SA provides a fully functional AIX volume manager integration script as a sample. During software provisioning, the script will create a temporary file system when it is run in the *pre-stage* phase.

SA will download software into the temporary file system. After the software has been installed, the file system will be deallocated when the script is run in the *post-action* phase.

Importing the LVM Script into SA

To use this script you must first import it into SA. Perform the following tasks.

1. Locate the file `aix-lvm-remediate-script.sh` on your SA product distribution media and save it to a local directory.
2. Log in to the SA Client.
3. Select **Library ➤ By Type ➤ Scripts ➤ Unix.**
4. Select the **Actions ➤ New**... menu item. The New Script window appears.
5. In the New Script window, provide the following information.

Table 2 LVM Script Information

Script Property	Instructions for Setting the Property
Name:	Set to `"Remediate:AIX LVM Integration"`.
Location:	Use the Select button to specify where in the SA library to save the script.
Changes Server?	Set to "Yes".
Run as super user:	Set to "Yes".
Script Contents:	Use the Import Script File button to open the `aix-lvm-remediate-script.sh` file you saved in step 1. Make sure to set Encoding: English (ASCII).
Description:	Set to "This script creates a temporary file system on AIX servers where remediate can download packages. After all packages have been installed, the file system is deallocated."

6. Select the **File ➤ Save** menu item.
7. Log out of the SA Client.

The script is now in the SA library and ready to use as described in the next section.

Using the LVM Script

Perform the following tasks on each AIX managed server where you want to use the script.

1. Log in to the SA Client.
2. Locate the Managed Server in the SA Client.
3. Double-click the server to display it in its own window.
4. Click **Custom Attributes**.

5 Select **Actions ➤ Add** or click the "+" button to add a new custom attribute. Name the first custom attribute `OPSWremediate_action_script` and *s*et its value to the name and location of the script in the SA Library, using "/" as the path separator. For example, if the script is in the root folder, use "`/Remediate:AIX LVM Integration`".

6 Select **Actions ➤ Add** or click the "+" button to add a new custom attribute. Name the second custom attribute `package_download_dir`. Its value is the mount point for the temporary file system created by `aix-lvm-integration.sh`. A suggested value is `/OPSWremediate_tmp`.

7 (Optional) Select **Actions ➤ Add** or click the "+" button to add a new custom attribute. Name the third custom attribute `OPSWremediate_action_script_args.` The `aix-lvm-integration.sh` script supports two arguments:

   a `-g <VolumeGroup>` — Specify a volume group from which to allocate the file system. The default is `rootvg`.

   b `-m <Size>` — Specify a minimum size in megabytes needed to create a temporary file system. For example, specifying 100 means that the total download size in a given remediate needs to exceed 100MB for the temporary file system to be created, otherwise remediate will just use the default location under `/var/opt/opsware/agent`.

8 The script time-out must be sufficient to allocate and deallocate a file system. If an AIX server takes longer than the default of one minute to complete the `crfs` and `mount` operations, you can use the `OPSWremediate_action_script_timeout` custom attribute to increase the time-out.

The script will be used whenever software is installed on the managed server. For more information, see "Software Management" in the *SA User Guide: Application Automation*.

Supported Platforms - General

In some cases, the list of supported platforms for managed servers in the SA documentation may not exactly match the platform support listed in these release notes.

For example, the virtualization, Service Automation Visualizer (SAV), and OS provisioning chapters in the SA user guides all list supported managed platforms, but some may not be consistent with the managed platforms list found in Chapter 2, Platform and Environment Support for SA 7.80, on page 23 of this guide. Please consult the platform support here for the latest information.