

# 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: 7.83

---

## Release Notes

Document Release Date: May 2010  
Software Release Date: May 2010



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

© Copyright 2000-2010 Hewlett-Packard Development Company, L.P.

### Trademark Notices

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

Java™ is a U.S. 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.

Adobe® is a trademark of Adobe Systems Incorporated.

## Documentation Updates

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

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

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

**<http://support.openview.hp.com/selfsolve/manuals>**

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

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

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

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

### Document Changes

Chapter	Date	Changes
	May 2010	Document Created

## Support

Visit the HP Software Support Online web site at:

**[www.hp.com/go/hpsoftwaresupport](http://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](http://h20230.www2.hp.com/new_access_levels.jsp)**



# Contents

1	New in SA 7.83	15
	Critical Defect Fixes	15
	Supported Operating Systems	19
	Revised Sizing Guidelines	20
	New Memory Requirement for Solaris x86_64 VM PXE Booting	20
	SA Cores on VMs Support	21
	New in 7.83	21
	New Supported Platforms — Managed Servers	21
	New Supported Platforms — SA Cores and Satellites	21
	New Supported Platforms — Virtualization	22
	New Product Integration	22
	Red Hat Enterprise Linux 4.x PPC64 and 5.x PPC64 OS Provisioning	22
	Red Hat Enterprise Linux 4.x PPC64 Sample Kickstart File	22
	Red Hat Enterprise Linux 5.x PPC64 Sample Kickstart File	23
	DHCP Configuration For PowerPC	23
	Network Booting Red Hat Enterprise Linux 4.x or 5.x PPC64 Servers	23
	SuSE Linux Kernels and PPC Architecture	24
	New JDK Version Required for the DCML Exchange Tool (DET)	24
	New in 7.82	24
	New Supported Platforms — Managed Servers	24
	New Supported Platforms — SA Core and Satellite	25
	Oracle Real Application Clusters (RAC) Support	25
	Solaris Patching Supports Patch Bundles	25
	Solaris Patching and Benign Error Codes	26
	Behavior when a Pre-Install Script Fails	27
	Approving Blocked Jobs that Run SA Extensions	28
	Enabling Job Approval for APXs	29
	Disabling Job Approval for APXs	29
	Restricting Access to RPM Folders	30
	How the RPM Folder Restrictions Work	30
	Enabling RPM Folder Restrictions	30
	Custom Attribute Format	30
	Examples	30
	Troubleshooting Errors	31
	New in SA 7.81	31
	Microsoft Hyper-V Virtual Machine Enhancements	31
	Solaris Patching Enhancements	32
	New Platform Support for Managed Servers	32
	Windows Agent Deployment Helper Obsolete	33

Agent Deployment Tool (ADT) Behavior in a Mixed-SA Version Environment .....	33
Veritas File System Support - Red Hat Enterprise Linux SA Cores .....	34
Storage Visibility and Automation Feature .....	34
Documentation for SA 7.83 .....	35
<b>2 Installing SA 7.83 .....</b>	<b>37</b>
SA 7.83 Core and Satellite Software Installation Procedure .....	37
General Information .....	37
Pre-Patching Procedures .....	39
Installation Procedure .....	40
Software Repository Content Upgrade .....	41
General Information .....	41
Upgrading the First Core Content .....	42
Rolling Back the Upgrade .....	42
Notes: .....	42
Rolling Back truth_create_local_dc_table.sh .....	42
Rolling Back truth_role_class_bridge.sh .....	43
Post-Patch Installation Tasks .....	43
Update SESSION_SERVICE_INSTANCES Table .....	43
Prerequisites .....	43
Running the truth_waypurge_sesstree_delete_max Script .....	44
Rolling Back the truth_waypurge_sesstree_delete_max Script Changes .....	44
Changes Made by truth_waypurge_sesstree_delete_max.sh .....	44
After Running the Script .....	45
Windows Server CLI Installation .....	46
<b>3 Fixed in SA 7.83 .....</b>	<b>47</b>
Fixed in SA 7.83 .....	47
Agents .....	47
QCCR1D 97923 .....	47
QCCR1D 98219 .....	47
QCCR1D 102321 .....	47
QCCR1D 103678/108387109467 .....	48
QCCR1D 104974 .....	48
QCCR1D 105363 .....	48
QCCR1D 106327 .....	48
QCCR1D 106621 .....	48
QCCR1D 106761 .....	49
QCCR1D 106983 .....	49
QCCR1D 107706 .....	49
QCCR1D 107958 .....	49
QCCR1D 108800 .....	49
QCCR1D 108801 .....	50
QCCR1D 109241 .....	50
Application Configuration .....	50
QCCR1D 96141 .....	50
QCCR1D 98407 .....	50
QCCR1D 102551 .....	51

QCCR1D 105927 .....	51
QCCR1D 106965 .....	51
Audit and Compliance .....	51
QCCR1D 107794 .....	51
QCCR1D 108376 .....	52
QCCR1D 108454 .....	52
QCCR1D 110370 .....	52
QCCR1D 110871 .....	52
Automation Platform Extensions (APX) .....	53
QCCR1D 105597 .....	53
Command Center .....	53
QCCR1D 107732 .....	53
Command Engine .....	53
QCCR1D 98445 .....	53
QCCR1D 102616 .....	53
Custom Extensions .....	54
QCCR1D 108148 .....	54
DCML Tool (DET) .....	55
QCCR1D 107377 .....	55
Global File System .....	55
QCCR1D 107483 .....	55
QCCR1D 109315 .....	55
Model Repository .....	56
QCCR1D 108378 .....	56
OS Provisioning .....	56
QCCR1D 93355 .....	56
QCCR1D 106181 .....	56
QCCR1D 107291 .....	56
QCCR1D 108110 .....	57
QCCR1D 108111 .....	57
QCCR1D 108113 .....	57
QCCR1D 109393 .....	57
Patch Management - Solaris .....	58
QCCR1D 102564 .....	58
QCCR1D 105981 .....	58
QCCR1D 107130 .....	58
QCCR1D 108503 .....	58
Patch Management - Unix .....	59
QCCR1D 107109 .....	59
QCCR1D 108222 .....	59
Patch Management - Windows .....	59
QCCR1D 107897 .....	59
SA Client .....	59
QCCR1D 109052 .....	59
SA Installer .....	60
QCCR1D 105675 .....	60

Search	60
QCCR1D 110005	60
Server Management - Managed Servers	60
QCCR1D 80776	60
QCCR1D 107142	60
QCCR1D 108074	61
Server Module (SMO)	61
QCCR1D 101980	61
QCCR1D 105810	61
Software Management	61
QCCR1D 99631	61
QCCR1D 102471	62
QCCR1D 106606	62
QCCR1D 106847	62
QCCR1D 107877	62
QCCR1D 108442	62
QCCR1D 108776	63
QCCR1D 109818	63
QCCR1D 110199	63
Web Services Data Access Engine	63
QCCR1D 105241	63
QCCR1D 107878	63
QCCR1D 109256	64
QCCR1D 109318	64
QCCR1D 110459	64
QCCR1D 110988	64
Fixed in SA 7.82	65
Agents	65
QCCR1D 98761	65
QCCR1D 101916	65
QCCR1D 102457	65
QCCR1D 103666	65
QCCR1D 103702	66
QCCR1D 104589	66
Audit and Compliance	66
QCCR1D 102870	66
Automation Platform Extensions (APX)	67
QCCR1D 82077	67
QCCR1D 91006	67
QCCR1D 91231	67
QCCR1D 97914	67
QCCR1D 100912	68
QCCR1D 103757	68
QCCR1D 103836	68
QCCR1D 106153	68
Command Engine	69
QCCR1D 97400	69



QCCR1D 102836 .....	69
QCCR1D 103175 .....	69
QCCR1D 103955 .....	69
Data Access Engine .....	70
QCCR1D 102962 .....	70
DCML Tool (DET) .....	70
QCCR1D 101734 .....	70
Distributed Scripts .....	70
QCCR1D 82714 .....	70
Extensible Discovery .....	70
QCCR1D 102187 .....	70
Global File System .....	71
QCCR1D 92767 .....	71
Installer .....	71
QCCR1D 100931 .....	71
QCCR1D 101197 .....	71
QCCR1D 106279 .....	72
OS Provisioning .....	72
QCCR1D 82514 .....	72
QCCR1D 92597 .....	72
QCCR1D 96317 .....	73
QCCR1D 96408 .....	73
QCCR1D 97493 .....	73
QCCR1D 98240 .....	73
QCCR1D 99477 .....	74
QCCR1D 99976 .....	74
QCCR1D 100476 .....	74
QCCR1D 102332 .....	74
QCCR1D 102341 .....	74
QCCR1D 102449 .....	75
QCCR1D 102830 .....	75
QCCR1D 103911 .....	75
QCCR1D 103913 .....	75
QCCR1D 104679 .....	76
QCCR1D 104764 .....	76
Patch Management - Solaris .....	76
QCCR1D 102345 .....	76
QCCR1D 103604 .....	76
Patch Management - SUSE Linux .....	77
QCCR1D 102109 .....	77
Patch Management - Unix .....	77
QCCR1D 83879 .....	77
QCCR1D 93840 .....	77
Patch Management - Windows .....	77
QCCR1D 102628 .....	77
QCCR1D 105637 .....	78

Red Hat Network Import . . . . .	78
QCCR1D 105106 . . . . .	78
QCCR1D 106016 . . . . .	78
Server Module . . . . .	78
QCCR1D 105360 . . . . .	78
Software Management . . . . .	79
QCCR1D 93946 . . . . .	79
QCCR1D 94106 . . . . .	79
QCCR1D 100046 . . . . .	79
QCCR1D 101517 . . . . .	80
QCCR1D 101673 . . . . .	80
QCCR1D 102650 . . . . .	80
QCCR1D 106460/101961 . . . . .	80
QCCR1D 106463/99524 . . . . .	80
Virtualization . . . . .	81
QCCR1D 103752 . . . . .	81
Web Services Data Access Engine . . . . .	81
QCCR1D 104013 . . . . .	81
Fixed in SA 7.81 . . . . .	81
Agents . . . . .	81
QCCR1D 82756 . . . . .	81
QCCR1D 92264 . . . . .	82
QCCR1D 93169 . . . . .	82
QCCR1D 93940 . . . . .	82
QCCR1D 98995 . . . . .	82
QCCR1D 100053 . . . . .	83
Application Automation Extensions (APXs) . . . . .	83
QCCR1D 93600 . . . . .	83
QCCR1D 99364 . . . . .	83
Application Configuration . . . . .	83
QCCR1D 93633 . . . . .	83
Audit and Compliance . . . . .	84
QCCR1D 73612 . . . . .	84
QCCR1D 97634 . . . . .	84
QCCR1D 90961 . . . . .	84
QCCR1D 94467 . . . . .	84
QCCR1D 98718 . . . . .	84
QCCR1D 99537 . . . . .	85
Command Engine (OCC) . . . . .	85
QCCR1D 83027 . . . . .	85
QCCR1D 100078 . . . . .	85
QCCR1D 84111 . . . . .	85
Custom Extensions . . . . .	86
QCCR1D 92622 . . . . .	86
Data Access Engine . . . . .	86
QCCR1D 95875 . . . . .	86
QCCR1D 99604 . . . . .	86

Gateways . . . . .	86
QCCR1D 93982 . . . . .	86
Global File System . . . . .	87
QCCR1D 100563 . . . . .	87
Model Repository . . . . .	87
QCCR1D 93757 . . . . .	87
QCCR1D 110310 . . . . .	87
Networking . . . . .	88
QCCR1D 92622 . . . . .	88
OS Provisioning . . . . .	88
QCCR1D 89237 . . . . .	88
QCCR1D 90094 . . . . .	88
QCCR1D 93128 . . . . .	88
QCCR1D 93847 . . . . .	89
QCCR1D 95918 . . . . .	89
QCCR1D 99603 . . . . .	89
Patch Management - Solaris . . . . .	89
QCCR1D 90961 . . . . .	89
QCCR1D 91806 . . . . .	90
QCCR1D 92173 . . . . .	90
QCCR1D 92426 . . . . .	90
QCCR1D 93225 . . . . .	90
Patch Management - Windows . . . . .	91
QCCR1D 79697 . . . . .	91
QCCR1D 83968 . . . . .	91
QCCR1D 90509 . . . . .	91
QCCR1D 92308 . . . . .	91
QCCR1D 93393 . . . . .	92
QCCR1D 93496 . . . . .	92
QCCR1D 94132 . . . . .	92
QCCR1D 97792 . . . . .	92
Powershell . . . . .	93
QCCR1D 90201 . . . . .	93
SA Client . . . . .	93
QCCR1D 92982 . . . . .	93
QCCR1D 93159 . . . . .	93
QCCR1D 94277 . . . . .	93
SAS Web Client . . . . .	94
QCCR1D 70583 (159229) . . . . .	94
Scripts . . . . .	94
QCCR1D 82714 . . . . .	94
Server Module . . . . .	94
QCCR1D 83143 . . . . .	94
QCCR1D 92829 . . . . .	94
QCCR1D 93173 . . . . .	95
QCCR1D 94119 . . . . .	95

QCCR1D 95403 .....	95
QCCR1D 99173 .....	95
Software Management .....	96
QCCR1D 72251 .....	96
QCCR1D 76594 .....	96
QCCR1D 88615 .....	96
QCCR1D 90586 .....	96
QCCR1D 93309 .....	97
QCCR1D 94127 .....	97
QCCR1D 94379 .....	97
QCCR1D 96839 .....	97
QCCR1D 97790 .....	98
QCCR1D 100395 .....	98
QCCR1D 100396 .....	98
QCCR1D 100417 .....	98
QCCR1D 100854 .....	98
Virtualization .....	99
QCCR1D 83067 .....	99
QCCR1D 89739 .....	99
QCCR1D 93055 .....	99
QCCR1D 93123 .....	99
QCCR1D 93220 .....	100
QCCR1D 93703 .....	100
QCCR1D 93756 .....	100
QCCR1D 94076 .....	100
QCCR1D 94207 .....	101
QCCRID 110493 .....	101
Visual Analyzer .....	101
QCCR1D 84313 .....	101
Web Services Data Access Engine .....	101
QCCR1D 83222 .....	101
QCCR1D 92819 .....	102
<b>4 Known Problems, Restrictions, and Workarounds in SA 7.83 .....</b>	<b>103</b>
Agents .....	103
QCCR1D 100660 .....	103
QCCR1D 102401 .....	103
Audit and Compliance .....	104
QCCR1D 102706 .....	104
Extensible Discovery APX .....	105
QCCR1D 106467 .....	105
Global File System .....	105
QCCR1D 93497 .....	105
Hyper-V .....	106
QCCR1D 97630 .....	106
QCCR1D 98310 .....	106

QCCR1D 101449 . . . . .	106
QCCR1D 102344 . . . . .	107
Model Repository . . . . .	107
QCCR1D 93757 . . . . .	107
QCCR1D 96568 . . . . .	108
QCCR1D 111642 . . . . .	109
OS Provisioning . . . . .	110
QCCR1D 93849 . . . . .	110
QCCR1D 101920 . . . . .	110
QCCR1D 102449 . . . . .	110
QCCR1D 111445 . . . . .	111
Patch Management: Solaris . . . . .	111
QCCR1D 95745 . . . . .	111
QCCR1D 98409 . . . . .	111
QCCR1D 100566 . . . . .	112
QCCR1D 101449 . . . . .	112
QCCR1D 104468 . . . . .	112
QCCR1D 106844 . . . . .	113
QCCR1D 111601 . . . . .	113
QCCR1D 111692 . . . . .	113
Patch Management: Unix . . . . .	114
QCCR1D 106847 . . . . .	114
Permissions . . . . .	114
QCCR1D 101710 . . . . .	114
SA Client . . . . .	114
QCCR1D 105630 . . . . .	114
Satellites . . . . .	115
QCCR1D 97659 . . . . .	115
Software Management . . . . .	115
QCCR1D 100754 . . . . .	115
Software Repository . . . . .	116
QCCR1D 99828 . . . . .	116
Virtualization . . . . .	116
QCCR1D 93492 . . . . .	116
<b>5 Documentation Errata . . . . .</b>	<b>117</b>
SA 7.82 Release Notes . . . . .	117
<i>SA Planning and Installation Guide</i> . . . . .	117
Chapter 1: SA Core Component Bundling (page 15) . . . . .	117
Chapter 2: Pre-Installation Requirements (page 55) . . . . .	117
Chapter 3: Solaris Requirements (page 48) . . . . .	118
Chapter 3: Pre-Installation Requirements, Table 18 (page 59) . . . . .	118
Chapter 3: SUSE Enterprise Server 10 Requirements . . . . .	119
Required SUSE Linux Enterprise Server 10 Packages . . . . .	119
Appendix A: Table 42 (Page 188) . . . . .	121
Appendix A: Solaris Requirements (page 190) . . . . .	121

Appendix A: Required and Suggested Parameters for init.ora (page 203) .....	121
Both Oracle 10g and 11g .....	121
Oracle 10g only .....	121
Oracle 11g only .....	122
Appendix A: Changing Kernel Parameter Values for Linux (page 198) .....	122
<i>SA Upgrade Guide</i> .....	122
Chapter 1: OS Provisioning Stage 2 Image Upload No Longer Required (page 8) .....	122
Chapter 3: Phase 1, Step 3b (page 46) .....	122
SA Policy Setter Guide .....	123
Incorrect Instructions: .....	123
Correct Instructions: .....	123
Users Guide: Application Automation, OS Provisioning, Manage Boot Clients (MBC) .....	123
Oracle RAC Support: Oracle Setup for the Model Repository/ <i>SA Planning and Installation Guide</i> , Appendix A .....	123
Supported Oracle Versions Matrix .....	124
Supported Oracle Versions: .....	124
Supported Operating Systems .....	124
Set up the Oracle RAC database/instances .....	124
Create the Database with the Required Initialization Parameters .....	124
Create the required table spaces .....	124
Required and Suggested Parameters for init.ora .....	125
Create the User opsware_admin .....	125
Installing the Model Repository .....	126
Model Repository Installation on a Remote Database (truth) RAC Server .....	127
Post SA installation process .....	132
Making changes to tnsnames.ora on the SA server .....	132
Making changes to listener.ora on one of the RAC node server (instance) .....	133
Vault.conf file changes .....	135
Upgrading the Model Repository .....	135
Planning and Installation Guide, First Core Post-Installation Tasks (page 121) .....	135
Edit the jboss_wrapper.conf File .....	135

# 1 New in SA 7.83

## Critical Defect Fixes

The following defects were fixed in SA 7.83:

**Table 1 Critical Defect Fixes in SA 7.83**

QCCRID	Description
80776	The Network Association box in the device group properties page appears unchecked even if the group is already associated to a network.
93355	When you use the <code>import_media</code> command to update an operating system installation media name that is already imported, the media name is not updated in the SAS Web Client.
96141	Editing errors occur when you create or modify rules in the Application Configuration Audit and Remediation editor.
97923	Although the Agent upgrade completes successfully, the Agent Upgrade Custom Extension software returns an unsuccessful upgrade error.
98219	When you try to import an exported comma-separated-values (CSV) file, you get the following error:  The following input records were incorrectly formatted and were skipped.
98407	When you use the <code>GroupConfigurable.pushConfiguration()</code> API call, you receive a null pointer exception.
98445	When you choose Tools ► Options in the Server Automation Client, the cursor becomes unresponsive.
99631	You cannot force a server to reboot during a software remediation if the Suppress Reboot option is enabled.
101980	If you scan a server for its runtime state, the software throws an exception and does not return any information.
102321	If you modify the default software policies, during a patch content upload, the Opware Agent Tools installer returns a missing software policies error instead of updating/creating the missing policy.
102471	The server clock and the core clock are not synchronized, so reported remediation times can be inconsistent because some devices use the server clock and some the core clock.
102551	In the Application Configuration Audit and Remediation tool, an entire rule is remediated if a part of that rule fails, but only the failed part should be remediated.

**Table 1 Critical Defect Fixes in SA 7.83 (cont'd)**

<b>QCCRID</b>	<b>Description</b>
102564	When you attempt to do an attach and remediate operation without first running the create_db script on the core, the software compliance scan status displays a Scan failed error.
102616	Environment variables in scripts do not always resolve as expected.
103678/109467	You cannot obtain device manufacturer/hardware information when you issue the bs_hardware command. Instead, the software displays the following system diagnostic message:  Hardware Stack Shape: Device IDs with unrepresented model_type: [239580100]
104974	SA Windows agent heartbeat thread starts later than it should.
105241	The AuthorizationService.findAuthorizedResources() API call/ authorization service fails for the OperationConstants.READ_USER operation, resulting in an Oracle error.
105363	RFE for SA 7.8x support in Chinese locale.
105597	An Automation Platform Extensions (APX) Program fails to run (from either a group or an All Managed Servers list) after you press the Start Job button in the last step.
105675	After a rollback from SA 7.82 to 7.80, the SA version is shown incorrectly. It still shows as 7.82 instead of 7.80.
105810	When you perform a runtime state scan of a server, it does not display the existing logged-in users.
105927	The Application Configuration tool copies files to the target location instead of moving them, causing some applications to return an error when they read a 0-byte configuration file.
105981	When remediating a Solaris patch bundle or a Solaris cluster, the value of the way.remediate.action_timeout parameter should be set to the highest value of the three values in the following parameters: way.remediate.solaris_cluster_package_alarm_timeout, way.remediate.action_timeout, and way.remediate.package_alarm_timeout. If the value of the way.remediate.action_timeout parameter is less than the value of the solaris_cluster_package_timeout, the way.remediate.action_timeout expires first, causing the job to time out.
106181	When you select an operating system installation profile in the SAS Web Client, the WinPE attributes are not displayed.
106327	Remediation operation fails because of excessive operation output coupled with low caller consumption rates. An unexpected error is returned.
106606	The import_aix_packages utility does not always properly detect patch files.
106621	You cannot perform an agent update using the Agent Upgrade tool due to an incompatibility between the tool and the current agent versioning scheme.



**Table 1 Critical Defect Fixes in SA 7.83 (cont'd)**

<b>QCCRID</b>	<b>Description</b>
106761	The software returns an unexpected traceback exception error when you set the Manage Software Policy to Read, and you use the <code>solpatch_import</code> command to create a policy.
106847	You receive an endless Invalid LPP file error when you try to import an AIX patch bundle.
106965	For partial templates, the Preserve Format menu option in the Application Defaults valueset editor only has the Yes value enabled. However, when you choose this option and save it, its value resets to a blank value.
106983	When you run a prerequisite installation check for the VMware ESXi server, the Agent performs the check and also begins to manage the server, although the Manage Server menu item is still enabled. The installation check should be disabled.
107109	During patch remediation, some AIX packages fail and display the following error: ValueError: invalid literal for int(): v>3
107130	After a new server is assimilated into the core, the applicability calculation incorrectly reports that bundles are non-applicable to the server, despite the fact that there is no software-registration data.
107142	You cannot change the value of the Server Use or Server Stage fields in the SA Client.
107291	Customer Request: WinPE HP iLO from SSTK driver request for HP DL 380 G6.
107377	Recurrence of bug with DCML (DET) command line utility.
107483	Users are not deleted from the user cache. Subsequently, those same users cannot access the OGFS because the system considers them re-created users.
107706	An agent running Python Version 1.5 cannot download a file that is greater than 2 GigaBytes (GB).
107732	You cannot create search criteria based on virtualization because the search text field gathers characters in reverse order.
107794	When you create hundreds of Register Software rules at a time during an audit, the run dialog and the audit log file display an out-of-memory (OOM) error.
107877	The yum wrapper fails to treat the <code>kernel-default-base</code> script as an install-only package.
107878	Import/Export packages time out in the SA Client if there is no direct access to port 443 of the Core Gateway.
107897	Windows agents fail to report installed BSA Essentials Network (BSAEN) patches that have software releases in the form: <code>/packages/any/nt/</code> .
107958	Cannot upgrade an agent that is installed on a Windows Server 2008 R2 x86-64.
108074	After you use the Manage Boot Clients (MBC) to set server stage and use fields, the Server Automation Client displays inconsistent field information, but the SAS Web Client and the OGFS display the correct information.
108110	If you run an Install Sequence job, scrolling is disabled in the Select Server and Preview Steps results.

**Table 1 Critical Defect Fixes in SA 7.83 (cont'd)**

<b>QCCRID</b>	<b>Description</b>
108111	When you run an operating system sequence job, detail panes of selected servers displayed in an active job window close unexpectedly and are difficult to reopen.
108113	When you run an Install Sequence job, you cannot sort in the resulting job-window table.
108222	Some notes do not display in the job-status details of the Server Automation output display when you install two patches and one patch supersedes the other.
108376	The HTTP server waits a few seconds before disconnecting after it has read remote configuration files. When you conduct configuration scans against a large number of servers (60 or more) with 60 or more managed configuration files, this HTTP-server behavior produces too many MAXIMUM timeouts on the individual scanned servers.
108387	You cannot obtain device manufacturer/hardware information when you issue the <code>bs_hardware</code> command. Instead, the software displays the following system diagnostic message:  Hardware Stack Shape: Device IDs with unrepresented model_type: [239580100]
108442	The Solaris package handler does not search the full custom attribute scope when it looks for the <code>SolarisAdminFile</code> custom attribute because the file is not attached to a device.
108148	There are no custom user-interface extensions (such as Change Password CX) that effect changes to the server in the Approval Integration engine.
108378	The Compliance Dashboard takes a long time to load, resulting in a high CPU load on the database server
108454	The graphical user interface in the SA Client freezes when you try to download a large audit result. After a longer than usual time, an audit result browser eventually displays the result.
108503	For Solaris 7.82/7.81 patches that are not yet imported, the user interface freezes when you click the Vendor Documentation link in the patch browser.
108776	When Python-based daemons run out of file descriptors, they stop serving requests because 32-bit programs that use standard input/output are limited to 256 file descriptors.
108800	Clicking close (X) on scanning window is not working.
108801	Clicking close (X) on Agent Deployment window is not working.
109052	You cannot add a device group to a User group's access-control list if the device group has the same name as an existing user for that User group.
109241	The Last Deployment Attempt Message in the Summary view is blank.
109256	Linking to RHEL audit policy throws <code>ORA-01795: maximum number of expressions in a list is 1000</code>
109315	Global File System produces an <code>OutOfMemoryError</code> (OOM) during a larger audit.

**Table 1 Critical Defect Fixes in SA 7.83 (cont'd)**

<b>QCCRID</b>	<b>Description</b>
109318	Audit jobs and snapshots of most of the servers are completed, but the results are not available. The audit results calculations are aborted with Oracle error: ORA-00060 : deadlock detected while waiting for resource.
109393	For HP iLO firmware versions 1.78 and 1.79, the Manage Boot Clients (MBC) for the server with HP iLO secure socket layer connections throws connection timeout errors when it retrieves details from the iLO interface
109818	If you select the Hold reboots until the end option, and then echo OPSW_REBOOT from a script in a software policy, the managed server does not reboot.
110005	Advanced searches failed to display a list of windows services for Windows 64-bit operating systems.
110199	The remediate servers operation (ServerService.startFullRemediateNow()) in the Server Automation WebServices/Data Access Engine does not work. There is no device identifier for the job, so the remediate operation to the agent does not occur.
110310	In SA 9.0 the Waypurge Garbage Collection PL/SQL code was modified to fix a bug that did not delete all the child records from the session_service_instances table.  The CORD bug backports the changes made in SA 9.0 into SA 7.80.03.
110370	Audit snapshot files are too large and take up too much storage room.
110459	You might experience performance issues in the dynamic-device group membership calculation if you run a large number of servers.
110493	In the SA Client, if you choose <b>Servers ► Virtual Server</b> panel, Solaris10 x86-64bit VMs are not listed in the Managed Server panel under their ESX servers, even if you perform a VMware VM refresh.
110871	Audit custom scripts either time out without producing a result (such as when the script is waiting for an input command) or enter an endless loops. Some compliance checks whose parameters have not been set experience the same phenomenon.
110988	Inefficient SQL inline views cause the Selector Manager to return SQL queries with a longer execution time than normal.

## Supported Operating Systems

For a complete list of supported platforms for SA 7.83 Cores, Agents, and Satellites, see *SA Supported Platforms* provided with the SA documentation. You can find updated versions of the *SA Supported Platforms* document on the HP Self Solve website. For information about deprecated operating systems, see your 7.80 *SA Planning and Installation Guide* or *SA Upgrade Guide*.

## Revised Sizing Guidelines

SA 7.80 and later have increased memory demands on the Slice Component bundle host(s). [Table 2](#) and [Table 3](#) provide the revised sizing guidelines:

**Table 2 Small-to-Medium SA Deployment (SA 7.80 and later)**

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

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

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

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

Managed Servers	SA Component Distribution by Server				
	Server 1*	Server 2*	Server 3*	Server 4*	Server 5*
<b>2000</b>	MR	Infra, Slice 0, OS Prov	N/A	N/A	N/A
<b>4000</b>	MR	Infra, Slice 0, OS Prov	Slice 1	N/A	N/A
<b>6000</b>	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	N/A
<b>8000</b>	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	Slice 3

\* Server Configuration: 8 CPU Cores, 8 GB RAM, 1 GB/s network

## New Memory Requirement for Solaris x86\_64 VM PXE Booting

In order to PXE boot Solaris x86\_64 VM, you must assign the Solaris VM one gigabyte memory or more.

## SA Cores on VMs Support

SA 7.80 added support for running SA Core Components within VMWare ESX Virtual Machine (VM) environments.

In the release notes, HP recommended that the Model Repository not be deployed to a VM and that the only supported installations were those in which the VM which supports the SA Core infrastructure was the sole VM.

The intent was to ensure that in conditions where overall performance was potentially a factor, SA performance could be isolated from the environmental impact of resource contention caused by other VMs. However, it was not intended to require that all SA Core on VM installations would always have exclusive domain of the ESX container.

To clarify:

- SA Core components are supported when executed within VMs provided you follow VMWare's best practices for managing resource allocation and overall workload to ensure that other VMs sharing the same ESX container do not significantly impact the performance available to the VM hosting the SA Core Components.
- To facilitate support of Infrastructure and Slice Component bundles on VMs, HP reserves the right to ask you to replicate any potentially performance related issues in an environment where the VM supporting the SA Core Components is the sole VM active within the ESX container.
- To facilitate support of the Model Repository on a VM, HP reserves the right to ask you to replicate any issues in an environment where the Model Repository is installed on a supported physical platform. Any issues resulting from interactions between the Oracle Database and the VM platform requiring interaction with Oracle technical support are your responsibility.

## New in 7.83

### New Supported Platforms — Managed Servers

- Red Hat Enterprise Linux 5.5 x86/x86\_64, Itanium 64-bit, PowerPC
- SUSE Linux Enterprise Server 10 U3 PowerPC
- SUSE Linux Enterprise Server 11 PowerPC
- CentOS 5.4 x86, x86\_64
- Novell Open Enterprise Server 2 SP2 for x86, x86\_64
- VMware ESX 3.5 U5
- Simplified Chinese Locale support for Windows Server 2000, 2003, and 2003 R2.

### New Supported Platforms — SA Cores and Satellites

- Red Hat Enterprise Linux 5.4 x86\_64
- Core and Satellite running on ESX 3.5 U5



---

SA 7.80 adds support for IP Multipathing and NIC bonding support for core and satellites and SAN support for SA Cores.

---

## New Supported Platforms — Virtualization

- VMware ESX 3.5 U5

## New Product Integration

- SE 6.2.1 connector
- BSAE 2.0

## Red Hat Enterprise Linux 4.x PPC64 and 5.x PPC64 OS Provisioning

While most OS Provisioning procedures are the same for Red Hat Enterprise Linux 4.x PPC64 and 5.x PPC64 as documented in the *SA Policy Setter's Guide* and the *SA User's Guide: Server Automation*, there are certain differences.

Red Hat Enterprise Linux 4.x PPC64 and 5.x PPC64 Kickstart files should be specified similarly to that shown in the sample files below:

### Red Hat Enterprise Linux 4.x PPC64 Sample Kickstart File

```
lang en_US.UTF-8
timezone --utc US/Pacific
reboot
text
install
bootloader --location=partition --driveorder=sda,sdb --append="console=hvsi0
rhgb quiet"
#zerombr yes

clearpart --drives=sda --initlabel
part prepboot --fstype "PPC PReP Boot" --size=4 --ondisk=sda
part /boot --fstype ext3 --size=100 --ondisk=sda
part pv.3 --size=0 --grow --ondisk=sda
volgroup VolGroup00 --pesize=32768 pv.3
logvol / --fstype ext3 --name=LogVol100 --vgname=VolGroup00 --size=1024 --grow
logvol swap --fstype swap --name=LogVol101 --vgname=VolGroup00 --size=1000
--grow --maxsize=5888

authconfig --enablesshadow --enablemd5
rootpw opsware

firewall --disabled
selinux --disabled

skipx

%packages
@Base
```

## Red Hat Enterprise Linux 5.x PPC64 Sample Kickstart File

```
lang en_US.UTF-8
timezone --utc US/Pacific
reboot
text
install
bootloader --location=partition --driveorder=sda,sdb --append="console=hvsi0
rhgb quiet"
#zerombr yes

clearpart --drives=sda --initlabel
part prepboot --fstype "PPC PReP Boot" --size=4 --ondisk=sda
part /boot --fstype ext3 --size=100 --ondisk=sda
part pv.3 --size=0 --grow --ondisk=sda
volgroup VolGroup00 --pesize=32768 pv.3
logvol / --fstype ext3 --name=LogVol100 --vgname=VolGroup00 --size=1024 --grow
logvol swap --fstype swap --name=LogVol101 --vgname=VolGroup00 --size=1000
--grow --maxsize=5888

authconfig --enablesshadow --enablemd5
rootpw opsware

firewall --disabled
key --skip
selinux --disabled

skipx

%packages
@Base
```

## DHCP Configuration For PowerPC

PowerPC machines must be booted using BOOTP which requires that the `dhcpdtool dynamic-bootp` flag is enabled in each range statement in the `dhcpd_subnets.conf` file.

The `dynamic-bootp` usage is:

```
range [ dynamic-bootp ] low-address [ high-address ];
```

For more information about `dhcp.conf` statement usage, see:

<http://www.daemon-systems.org/man/dhcpd.conf.5.html>

## Network Booting Red Hat Enterprise Linux 4.x or 5.x PPC64 Servers

- 1 Mount the new PowerPC server in a rack and connect it to the network. The installation client on this network must be able to communicate with the SA DHCP server on the SA Core network. If the installation client is running on a different network than the SA Core network, your environment must have a DHCP proxy (IP helper).
- 2 Use the SMS menu to configure the server to boot from the hard disk on which the operating system will be installed because the OS Provisioning process requires several reboots that default to the local disk.

- 3 Start Open Firmware.
- 4 Use the boot command to boot the server over the network. This command requires the Open Firmware path to the device you are booting from. You can specify device aliases to a device's Open Firmware path. If you configured the boot order with the SMS menu you can use the `printenv` and `devalias` commands to create the alias.

For example:

```
printenv boot-device
boot-device /pci@800000020000002/pci@2,4/pci1069,b166@1/scsi@1/sd@5,0
/pci@800000020000002/pci@2/ethernet@1:speed=auto,duplex=auto,
192.168.157.2,,192.168.157.25,192.168.157.1

devalias net /pci@800000020000002/pci@2/ethernet@1
```

- 5 After you have set the net device alias, issue the following command:

```
boot net:[SERVER_IP],[IMAGE_FILE],[CLIENT_IP],[GW_IP] [ARGUMENTS]
```

You need only specify the `IMAGE_FILE` argument, for example:

```
boot net:,yaboot,,
```

Executing this command retrieves the bootloader (`yaboot`) and displays the server boot options. Press Enter to boot the default option (`linux5`) or wait for the boot to occur automatically.

- 6 The Red Hat Anaconda installer starts. If your server has multiple network interfaces, the installer may prompt you to specify the interface to use.
- 7 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 SAS Web Client Server Pool list.
- 8 (*Optional*) Record the MAC address and/or the serial number of the server so that you can locate the server in the SAS Web Client Server Pool list or in the SA Client Unprovisioned Servers list.
- 9 Verify that the server appears in the SA Client Unprovisioned Server list and is ready for OS installation. For more information, see the *SA User's Guide: Application Automation*.

## SuSE Linux Kernels and PPC Architecture

When installing SUSE Enterprise Linux on PPC architectures, consoles may not work after the operating system loads during the boot process. Therefore, when provisioning or reprovisioning a server with SUSE Enterprise Linux on PPC architectures, you could lose console access to the server being provisioned.

## New JDK Version Required for the DCML Exchange Tool (DET)

As of SA 7.80, the DCML Exchange Tool (DET) requires jdk 1.6.

## New in 7.82

### New Supported Platforms — Managed Servers

SA 7.82 added support for the following managed server operating systems:



- Red Hat Enterprise Linux 5.4
- Red Hat Enterprise Linux 5.2-5.4 Power
- Solaris 10 U8
- SuSE Linux Enterprise Server 10 SP3
- VMware ESX 4 U1

## New Supported Platforms — SA Core and Satellite

Core and Satellite components are now supported on SuSE Linux Enterprise Server 10 SP3.



For more detailed information on the latest supported platforms for the Server Automation product, see the HP software manuals site at <http://h20230.www2.hp.com/selfsolve/manuals>.

## Oracle Real Application Clusters (RAC) Support

Concurrent with the release of version 7.83, SA provides support for Oracle RAC. In order to configure SA for Oracle RAC support, you must perform a fresh installation of SA 7.80, configured for Oracle RAC, then upgrade to SA 7.82. For more information about configuring SA for Oracle RAC support, see [Oracle RAC Support: Oracle Setup for the Model Repository/SA Planning and Installation Guide, Appendix A](#) on page 123 of these release notes.

## Solaris Patching Supports Patch Bundles

Version 7.82 of HP Server Automation adds support for Solaris patch bundles.

- You can download Solaris patch bundles and import them into the SA library using the `solpatch_import` command. You can import each part of a bundle separately, but you cannot install the bundle until all the parts have been imported into the SA library. The Contents view in the SA Client displays the parts in the bundle. The bundle icon in the SA Client will be grayed out until all the parts have been imported. Note that you cannot import patch bundles using the Import Software menu item in the SA Client.
- You can install Solaris patch bundles directly on managed servers or on all servers in a device group or you can add Solaris patch bundles to a Solaris patch policy (or to a software policy), attach the policy to managed servers or device groups and then remediate the servers against those policies. When you remediate the servers or device groups, the Solaris patches specified in the attached policy are automatically installed on the managed servers.
- All `solpatch_import` actions, except the policy action, now can be performed with patch bundles.
- When you import a bundle, SA updates the metadata in the SA Library with all the patches contained in the bundle. Depending on the number of patches in your SA Library, the bundle import may take some time.
- Deleting a patch bundle from the SA Library or by using the `solpatch_import` command deletes all the parts of the bundle.
- The default reboot settings for patch bundles are listed below. You can change these settings by opening the patch bundle in the SA Client, selecting the Properties view and editing the Install Parameters.
  - Reboot Required: Yes – This setting indicates the managed server will be rebooted when the patch bundle is successfully installed.

- Install Mode: Single User Mode – This setting indicates that the patch bundle will be installed in single user mode. Note that the Solaris system is rebooted to single user mode, then the patch bundle is installed, then the system is rebooted to multiuser mode.
- Reboot Type: Reconfiguration – This setting indicates that a reconfiguration reboot will be performed after installing the patch bundle.
- Reboot Time: Immediate – This setting indicates that the server will be rebooted immediately after installing the patch bundle.
- A Solaris patch compliance scan will indicate that the server is out of compliance even though the patch bundle installed successfully if one or more patches in the bundle were not installed because a required prerequisite patch was not installed. For details on what patches in the patch bundle were not installed, see the log file for the patch bundle installation job.

A software compliance scan will similarly indicate the server is out of compliance if the patch bundle is included in the software policy and the same scenario occurs.

To bring the server into compliance, place the relevant patches into a patch policy, resolve the dependencies on the policy to place all required patches in the policy and remediate the policy on the server.

- You must set the “Manage Packages” permission to “Read and Write” to use the `solpatch_import` command. This is in addition to the permissions described in “Patch Management for Solaris” in the *SA User’s Guide: Application Automation*. For details on permissions, see the *SA Administration Guide*.
- If you encounter errors when importing Solaris patch bundles, perform the following troubleshooting steps.
  - a Log in as root to an SA core where the SA 7.82 patch has been installed.
  - b Locate the log file from the 7.82 patch install which is typically under `/var/log/opsware/install_opsware/patch_opsware.<time stamp>.log`
  - c Search this log file for a message with “update\_supplements.” For example, you could use the following `grep` command:
 

```
grep update_supp patch_opsware*
```
  - d The result should be a log message with “update\_supplements successfully completed”. However, if the message indicates the `update_supplements` failed, update the Solaris patch supplement file manually as follows.
  - e Log in as root to an SA core system where the `solpatch_import` command is installed.
  - f Change to the directory where the `solpatch_import` command is, `/opt/opsware/solpatch_import/bin`.
  - g Run the following command:
 

```
./solpatch_import -a update_supplements
```
  - h Try importing Solaris patch bundles again.

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

## Solaris Patching and Benign Error Codes

Installing Solaris patches sometimes results in benign error codes. A benign error code is an error code that does not reflect a true error situation. For example, a patch installation may fail because the patch is already installed or because a superseding patch is installed, resulting in a benign error code. The exit code from the Solaris `patchadd` command would indicate an error, when in reality the patch was not installed for a valid reason.

When a patch does not install because of a true error situation such as the server being out of disk space, SA reports the error and the valid error code.

SA detects benign error codes and reports success in most cases. In the following two cases, however, Solaris cannot detect benign error codes:

- Solaris Deferred-Activation Patches
- Any patches installed on Solaris Global Zones where Local Zones are defined.

You can configure SA to detect benign error codes in these cases by performing the following steps.

- 1 Install the following patches on all your servers running Solaris 10:
  - 119254-36 (sparc)
  - 119255-36 (i386)
- 2 Run the SAS Web Client and log in as a user with “Configure Opsware” permission.

The Configure Opsware permission is given by default to the “SA/Opsware System Administrators” group. You can locate and set it in the SAS Web Client by selecting Administration ► Users & Groups, select the Groups tab, select the “SA/Opsware System Administrators” group and select the Features tab.
- 3 Under the Administration node, select System Configuration.
- 4 Select Command Engine.
- 5 In the configuration parameters table, locate the line “way.remediate.sol\_parse\_patchadd\_output”.
- 6 Select “Use value:”.
- 7 Enter the number 1 in the edit field.
- 8 Select the Save button.

## Behavior when a Pre-Install Script Fails

You can specify pre-install scripts in patches, packages and software that run before the patch, package or software is installed on a server. For each pre-install script, you can specify the behavior if the pre-install script fails. The following shows a pre-install script and the error setting.

**Figure 1 Error Behavior Setting for a Script**

**Install Scripts**

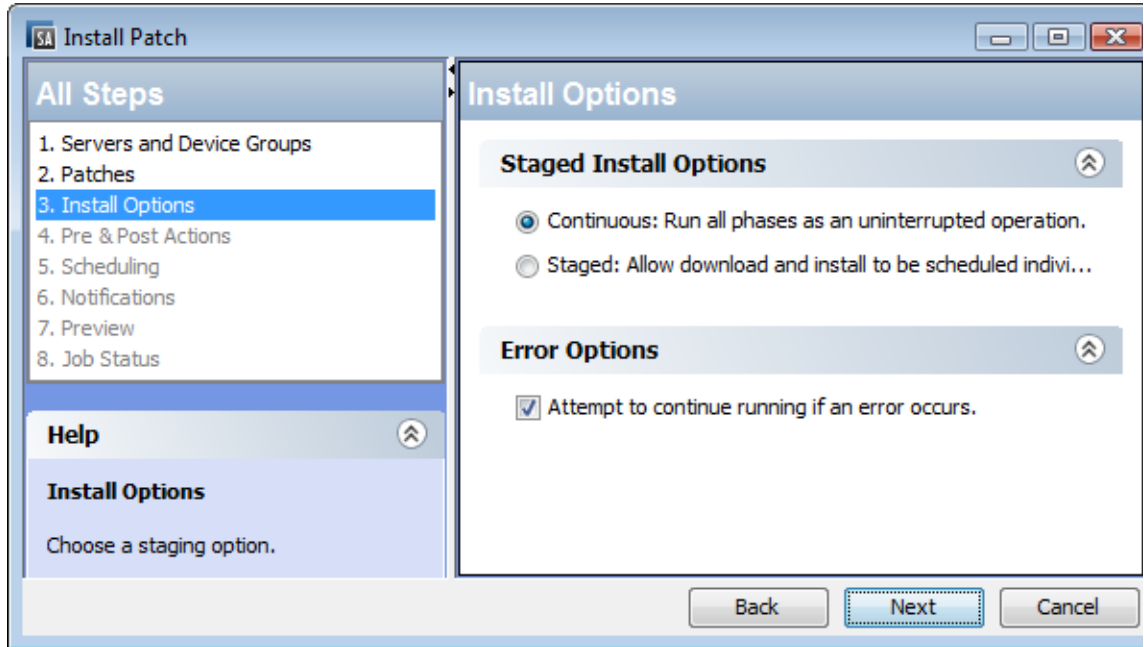
Pre-Install Script | Post-Install Script

```
RMFOLDER=/opt/opsware/dbfile.db
if [ -d $RMFOLDER ]; then
  rm -rf $RMFOLDER
fi
```

If Script Returns an Error:  Stop Install  Continue

When you initiate a remediate job or an install job that installs patches, packages or software, you can specify the behavior if any part of the job fails. The following shows an Install Patch job and the setting that controls the behavior when any part of the job fails.

Figure 2 Error Behavior Setting for an Install Patch Job



Before SA 7.82, if the error setting for the job specified “Attempt to continue running if an error occurs” and the error setting for the pre-install script specified “Stop Install” and an error occurred in the pre-install script, the job would ignore the script’s error setting and continue running.

As of SA 7.82, if this situation occurs, the error setting for the pre-install script applies and the patch or package or software will not be installed. The job will continue running and attempt to install the remaining patches, packages or software.

To retain the pre-SA 7.82 behavior, simply change the error setting on the pre-install script to “Continue”.

## Approving Blocked Jobs that Run SA Extensions

Job Approval Integration in SA allows you to block certain SA jobs from running until they are verified and unblocked. The typical method of unblocking these blocked jobs is by using HP Operations Orchestration (OO). SA 7.82 provides a way to unblock jobs that run program APXs (Automation Platform Extensions) without requiring HP Operations Orchestration. For more information on Job Approval Integration, see the *SA Platform Developer’s Guide*.

In releases prior to SA 7.82, the only way to unblock blocked jobs was by calling an OO flow. The OO flow performed the appropriate checks and unblocked the job, allowing it to run.

SA 7.82 adds the ability to verify and unblock jobs that run program APXs without requiring HP Operations Orchestration.



This applies only to “Run Program Extension” jobs, which are jobs that run a program APX. APXs are extensions to SA. For more information on APXs, see “Creating Automation Platform Extensions (APX)” in the *SA Platform Developer’s Guide*.

With SA 7.82, you can create a specifically named program APX that will run without blocking. This allows you to write a program APX that can unblock other APX jobs, without the control APX itself being blocked. To specify an APX to unblock jobs, set the following system configuration parameters in the SAS Web Client.

**Table 4 System Configuration Parameters for an APX to Unblock Jobs**

System Configuration Parameter	Value
approval_integration.apx.enabled	0 (default) disables the ability to unblock jobs with an APX. 1 enables unblocking jobs with an APX.
approval_integration.apx.uniquename	Specifies the name of the program APX that will handle blocked jobs.

## Enabling Job Approval for APXs

You must have the appropriate permissions to make changes to System Configuration parameters. For more information on permissions, see the *SA Administration Guide*.

To create this type of APX, perform the following steps:

- 1 Write a program APX that checks the blocked jobs and unblocks them using the SA API methods `approveBlockedJob()`, `updateBlockedJob()`, `cancelScheduledJob()` and `findJobRefs()`. These methods are the callbacks into SA that enable job approval integration. For details on writing APXs see “Creating Automation Platform Extensions (APX)” in the *SA Platform Developer’s Guide*.
- 2 Log in to the SAS Web Client. For more information on the SAS Web Client, see the *SA User’s Guide: Server Automation*.
- 3 In the navigation pane, select Administration System Configuration. This displays the subcomponents of the SA platform.
- 4 Under “Select a Product:”, select Opsware. This displays the system configurations you can modify.
- 5 Locate the entry for `approval_integration.apx.enabled`.
- 6 Under the Value column, select the “Use value” button.
- 7 In the text box next to the “Use value” button, enter a 1.
- 8 Locate the entry for `approval_integration.apx.uniquename`.
- 9 Under the Value column, select the “Use value” button.
- 10 In the text box next to the “Use value” button, enter the unique name of your program APX that checks and unblocks blocked jobs.
- 11 Select the Save button at the bottom of the page.
- 12 Set up a mechanism to run this APX. For example, you could schedule this APX to run periodically to check for blocked APXs.

## Disabling Job Approval for APXs

You must have the appropriate permissions to make changes to System Configuration parameters. For more information on permissions, see the *SA Administration Guide*.

To disable the unblocking APX, set the value of `approval_integration.apx.enabled` to 0. For details on setting this system configuration value, see [Enabling Job Approval for APXs](#) on page 29.

## Restricting Access to RPM Folders

In SA 7.82, you can ensure that your Linux managed servers only have access to the set of RPMs in the SA Library that apply to each server. You simply specify in a custom attribute the folders in the SA Library that the server has access to. All other folders will be inaccessible to the server. This section describes how to set up these restrictions.

With this new mechanism, you can mimic the common Redhat systems administration paradigm of having multiple, distinct yum (Yellowdog Updater, Modified) repositories. This gives you folder-level control over which versions of RPMs can be applied to a given server, allowing you to precisely manage platform update versions, for example Redhat Advanced Server AS4 Update 5 versus Update 6.

This is not intended as a user-level access control mechanism, but rather to restrict the library and folder view of a managed server from access to the full set of RPMs in the SA Library. For information on user level folder access controls and folder permissions in the SA Library, see the *SA Administration Guide*.

### How the RPM Folder Restrictions Work

During remediation, if a server has one or more of these custom attributes defined, SA reads the custom attribute values and only allows the managed server access to the RPMs in the SA Library folders specified in the custom attributes and their subfolders. Subfolders of all the specified folders are recursively searched for RPMs. All other folders are not accessible to the server.

### Enabling RPM Folder Restrictions

To restrict a server or group of servers to a subset of RPMs in the SA Library, set a custom attribute in the format described below on your managed server or at a location that will be inherited by the server such as a device group, a software policy, a customer, a facility and so forth.

These custom attributes follow the custom attribute inheritance rules. For example, if you set a custom attribute at the facility level, the servers in that facility will inherit the custom attributes.

SA does not validate the SA Library folder paths you specify in these custom attributes so make sure the folder paths you specify are correct.

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

### Custom Attribute Format

The custom attributes that restrict access to RPMs must be in the following format:

```
repo.restrict.<name>
```

Where <name> is any user-defined alphanumeric string. Specify a <name> that is descriptive and helps you remember the purpose of the custom attribute. You can define multiple custom attributes as long as each <name> is unique.

### Examples

The following defines custom attributes that grant access only to the SA Library directories /Redhat/AS4/en/x86\_64/U5 and /Oracle/10/AS4/x86\_64:

```
repo.restrict.as4u5=/Redhat/AS4/en/x86_64/U5
repo.restrict.oracle_updates=/Oracle/10/AS4/x86_64
```

The custom attribute value can be multiple lines. The following defines custom attributes that grant access only to the SA Library directories listed:

```
repo.restrict.as4u5=/Redhat/AS4/en/x86_64/U5
    /Redhat/AS4/en/x86_64/U5-extras
repo.restrict.s5u3=/Redhat/5Server/en/x86_64/U3
    /Redhat/5Server/en/x86_64/U3-extras
    /Redhat/5Server/en/x86_64/U3-VT
    /Redhat/5Server/en/x86_64/U3-Cluster
```

## Troubleshooting Errors

If you attempt to remediate a software policy that contains RPMs that are not accessible to the server, the following error message will be given:

```
The metadata needed to install this package is missing.
```

This indicates that SA was unable to access the RPM because the server does not have access to the RPM in the SA Library. To resolve this error, check the folder locations you have set in your custom attributes to ensure they are correct.

## New in SA 7.81

### Microsoft Hyper-V Virtual Machine Enhancements

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

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

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

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

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

- Memory size
- The number of virtual processors
- BIOS order
- VLAN and MAC address configuration of network adapters

- Media specification for DVDs
- Controller and location for virtual hard disks

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

## Solaris Patching Enhancements

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

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

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

## New Platform Support for Managed Servers

Table 5 lists all new operating system support for managed servers in SA 7.81.

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

**Table 5 Platform Support for Managed Servers in SA 7.81**

Operating System	Version
Windows	Windows Server 2008 R2 (Standard, Enterprise, Datacenter) Windows Server 2008 (Standard, Enterprise, Datacenter, Web)
CentOS	CentOS 5
Oracle	Oracle Enterprise Linux 5
Linux	SuSE Linux Enterprise Server 11
Sun	Solaris 10 U7
VMware	ESX Server 4.0 ESXi Server 4.0 Embedded ESXi Server 4.0 Installable



## Windows Agent Deployment Helper Obsolete

In SA 7.83, the *Windows Agent Deployment Helper (WADH)* is no longer required to manage Windows servers with SA and has been removed from the SA distribution. The process of bringing Windows servers under SA management is now the same as for any other platform.



---

After you install this patch on all your core and satellite servers and are certain that you will not need to roll back the 7.83 patch, you can redeploy the Windows server that hosted the WADH.

---

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

- The WADH installation instructions described under “Enabling ODAD for Windows Servers” on pages 118-119 of the 7.80 *SA Planning and Installation Guide* are no longer required.

- The bullet on page 35 of the *SA Policy Setter’s Guide* that reads:

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

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

is no longer valid. This change also affects online help.

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

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

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

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

When you run the Agent Deployment Tool (ADT) from a 7.83 SA Client session (the SA version of the core the SA Client session is logged in to), Windows agent deployment from that session is supported only to realms also running SA 7.83; deployment to realms running earlier SA versions is not supported.

If the SA Client session is logged into a pre-7.83 core (for example, 7.80, 7.50.03, etc.) as long as that SA core has a properly configured Windows Agent Deployment Helper server, you can deploy Windows agents from that session to realms running SA 7.83 as well as earlier versions.

## Veritas File System Support - Red Hat Enterprise Linux SA Cores

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

## Storage Visibility and Automation Feature

For Server Automation 7.83, the following changes were made to the Storage Visibility and Automation feature:

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

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

# Documentation for SA 7.83

The following documentation are provided with this patch release:

- *SA Release Notes for 7.83*
- *SA Supported Platforms*

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

- *SA Planning and Installation Guide*
- *SA Upgrade Guide*
- *SA Oracle Setup for the Model Repository*
- *SA Administration Guide*
- *SA Policy Setter's Guide*
- *SA User's Guide: Application Automation*
- *SA User's Guide: Server Automation*
- *SA Platform Developer's Guide*
- *SA Content Utilities Guide*
- *SA Content Migration Guide*
- *SA Open Source and Third-Party Software Acknowledgements*



## 2 Installing SA 7.83

This section describes the SA 7.83 installation procedure.

### SA 7.83 Core and Satellite Software Installation Procedure

#### General Information

- SA 7.83 can be rolled back, but only to the previous full release, SA 7.80.
- The `patch_opsware.sh` script is used both for installing and for uninstalling SA 7.83.
- There's no need to supply a response file with `patch_opsware.sh`.
- This patch includes updated Server Agents that will be uploaded to the Software Repository. However, no agents will be upgraded on core machines (that is, in the Model Repository) or on Managed Servers without manual intervention
- SA 7.83 can only be installed on systems running SA versions with a Build ID of `opsware_37.0.3006.*`.

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

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

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

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

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

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

```
%opsware_patch  
build_id: opsware_37.0.3826.0
```

- Before a patch operation (such as install/upgrade/uninstall), all core/satellite services must be up and running. If any services are stopped or dysfunctional (as reported by the `/etc/init.d/opsware-sas status` command), the patch operation will terminate.
- Upon completion of a patch operation, all services on the core/satellite machine should be up and running.
- If you are patching a multi-host core/satellite, you must patch each core and satellite host separately, one at a time.
- If you are patching a Multi-master mesh, HP recommends that you patch the primary core first, followed by secondary cores and satellites, thus ensuring that the primary core is at a higher version (such as SA 7.83 or higher) than the secondary cores.

If you must roll back the SA 7.83 patch in a Multi-master Mesh, HP recommends that you roll back the secondary cores and satellites first, then the primary core.

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

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

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

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

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

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

Please copy the certificate from another core machine (such as `occ`) to `/var/opt/opsware/crypto/oi`

and retry this operation.

- The following error may occur during upgrade on cores on which Solaris patching has not yet been set up:

```
You don't have permission to update the patch meta database in HP SA.
```

```
Please re-run this command with a proper hpsa_user and hpsa_pass.
```

```
The hpsa_user needs permission to write the folder
```

```
"/Opsware/Tools/Solaris Patching" and the Package Management
```

```
Client Feature, "Manage Package" permission set "Read & Write".
```

```
There was a problem with running update_supplements.
```

```
Please refer to section Patch Management for Solaris of the Users Guide:
```

```
Application Automation manual for details on how to set up Solaris patching on your core.
```

You can safely disregard this error.

## Pre-Patching Procedures

There are three pre-patching procedures you must complete before applying the 7.83 patch.

### 1 *Managed Platform Update*

You must install an SA update on 7.80 cores before installing the SA 7.83 patch. If you are upgrading from SA 7.81 or 7.82, this update will have already been installed. This update enables the SA Core to handle new supported managed platforms introduced in CORD patch releases by ensuring mesh compatibility between a First Core patched with SA 7.83 and unpatched Secondary Cores.

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



---

This update cannot be rolled-back.

---

- a To install the pre-patch update, run the following script:

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

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

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

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

```
/opt/opsware/occlient/ngui.jar checksum = <current MD5 checksum>
```

```
Patch not applicable
```

### 2 *Create New Table Update*

- a Log in as root on the Model Repository host and run the following script that creates a required Oracle database table. You will need to know the truth user password:

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

- b Restart Web Services Data Access Engine (twist) so that it is aware of the new table.

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



---

After running the `truth_create_local_dc_table.sh` script to create the `LOCAL_DC_TABLE`, you may see the following error when running the System Diagnostic test on your core:

```
Test Name: Model Repository Schema
Description: Verifies that the Data Access Engine's version of the schema
matches the Model Repository's version.
Component device: Data Access Engine (spin)
```

```
Test Results: The following tables differ between the Data Access Engine and
the Model Repository: local_data_centers.
```

This error is incorrect and you can disregard it.

---

### 3 *Create a New Table and Associated PL/SQL Objects*

- The Model Repository database (Oracle) must be running, other SA components can be shut down.
- You will need to copy two script files and two SQL files:

- truth\_role\_class\_bridge.sh
- truth\_role\_class\_bridge.sql
- truth\_role\_class\_bridge\_rollback.sh
- truth\_role\_class\_bridge\_rollback.sql

which are provided with the SA patch distribution in the directory:

<distro>/opsware\_installer/tools

Copy these files to any directory on the Model Repository host or host on which the Model Repository (Oracle) database is running, for example, to /var/tmp.

- You will need the following information:

- ORACLE\_HOME
- ORACLE\_SID
- The password for the schema owner TRUTH.

The script will prompt you for this information.

- You must run the script as root .

To run the script, issue the command in the form:

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

For example:

```
./truth_role_class_bridge.sh /u01/app/oracle/product/10.2.0/db_1 truth
```

## Installation Procedure

Perform the following tasks to install SA 7.83:

- 1 Mount the SA 7.83 distribution. Invoke `patch_opsware.sh` on every host in the core/satellite facility:

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

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

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

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

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

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



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

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

The installer displays the following upon completion:

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

## Software Repository Content Upgrade

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

### General Information

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



---

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

---

## Upgrading the First Core Content

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

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

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

The following menu is displayed:

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

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

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

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

## Rolling Back the Upgrade

To rollback SA 7.83 to SA 7.80, invoke the script:

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

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

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

### Notes:

- Rolling back SA 07.80 does not remove the Windows Server 2008 data that was created when the core was upgraded. For example, any Windows Server 2008 patches or policies created will remain. If you try to install these patches or attach the policies, an error will occur.
- Rolling back SA 7.80 does not delete any patches and policies that you have imported or created after the upgrade and these may fail with an error if you attempt to run them.

### Rolling Back `truth_create_local_dc_table.sh`

If, as part of a CORD rollback, you must rollback the table created by the `truth_create_local_dc_table.sh` script:

- a Stop the Web Services Data Access Engine (twist).

- b Log in as root on the Model Repository host and run the following rollback script. You will need to know the truth user password:

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

- c Restart Web Services Data Access Engine (twist) so that it is aware of the new table.

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

## Rolling Back truth\_role\_class\_bridge.sh

If, as part of a CORD rollback, you must rollback the changes made by the truth\_role\_class\_bridge.sh script, use the truth\_role\_class\_bridge\_rollback.sh script in the format:

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

For example:

```
./truth_role_class_bridge_rollback.sh /u01/app/oracle/product/10.2.0/db_1 truth
```

# Post-Patch Installation Tasks

## Update SESSION\_SERVICE\_INSTANCES Table

In SA 7.83 the Garbage Collection was modified so that all child records are completely deleted from the SESSION\_SERVICE\_INSTANCES table which improves performance.

After you have upgraded to SA 7.83, you should perform the following tasks to complete the update to the SESSION\_SERVICE\_INSTANCES table. You will run a script that will delete any existing child records in your SESSION\_SERVICE\_INSTANCES table which reduces the size of the table.



---

HP highly recommends, though it is not mandatory, that you perform the following tasks after upgrading to SA 7.83 in order to take advantage of the significant performance gains this can provide.

---

### Prerequisites

- The script must be run on all Model repository (truth) hosts.
- The script can be run on a working core.
- All Core components can be running.
- You must run the script as root .
- There are two scripts in the following directory:

```
<distro>/opsware_installer/tools/truth_waypurge_sesstree_delete_max/
```

```
— truth_waypurge_sesstree_delete_max.sh
```

```
— truth_waypurge_sesstree_delete_max_rollback.sh
```

Copy all files in that directory to any directory on the system where the Model Repository database is running, for example, to /var/tmp.

## Running the `truth_waypurge_sesstree_delete_max` Script

You will run a script called `truth_waypurge_sesstree_delete_max.sh` which removes the child records. There is also a script that rolls back the changes, see below.

Before running this script ensure that you have the following information:

- `ORACLE_HOME`
- `ORACLE_SID`
- The password for the schema owner `LCREP` and `GCADMIN`. The script prompts you for this information.

### Usage:

Invoke the script as follows:

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

For example:

```
./ truth_waypurge_sesstree_delete_max.sh /u01/app/oracle/product/10.2.0/db_1 truth
```



---

You can run this script multiple time without issue.

---

## Rolling Back the `truth_waypurge_sesstree_delete_max` Script Changes

If necessary, you can roll back changes made by `truth_waypurge_sesstree_delete_max.sh`.

To do so, you use the `truth_waypurge_sesstree_delete_max_rollback.sh` script. For example:

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

## Changes Made by `truth_waypurge_sesstree_delete_max.sh`

Changes made by the `truth_waypurge_sesstree_delete_max.sh` script include:

- 1 A new row `WAY_GC_SESSIONTREES_DELETE_MAX` is added to the `lcrep.audit_params` table.

To view the new row you can use the following SQL\*Plus command.

```
SQLPLUS> col NAME format a30
SQLPLUS> col AUDIT_PARAM_ID format a15
SQLPLUS> col VALUE format a30
SQLPLUS> set line 100
SQLPLUS> select AUDIT_PARAM_ID, NAME, VALUE from audit_params;
```

### Sample output:

```
AUDIT_PARAM_ID  NAME VALUE
-----
68 DAYS_WAY 30
69 DAYS_CHANGE_LOG 180
70 LAST_DATE_WAY 20-FEB-10
71 LAST_DATE_CHANGE_LOG 23-SEP-09
72 DAYS_AUDIT_LOG 180
73 LAST_DATE_AUDIT_LOG 23-SEP-09
74 WAY_GC_SESSIONTREES_DELETE_MAX 100 -----> new row
```

- The `truth_waypurge_sesstree_delete_max.sh` script also updates Waypurge Garbage collection PL/SQL code.

## After Running the Script

The following steps must be run on all Model Repository hosts after the script is run.

- Verify how many records are expected to be deleted.

```
SQLPLUS> SELECT count(session_id) FROM sessions
        WHERE (parent_session_id IS NULL OR
               parent_session_id IN (SELECT session_id FROM sessions WHERE
               parent_session_id IS NULL AND status = 'RECURRING')) AND
               status <> 'PENDING' AND status <> 'RECURRING' AND
               trunc(nvl(signoff_dt, nvl(end_dt, start_dt))) <
               (trunc(sysdate) - (SELECT value FROM audit_params WHERE name = 'DAYS_WAY'))
               AND NOT EXISTS (SELECT reconcile_session_id FROM device_role_classes
               WHERE reconcile_session_id IS NOT NULL AND
               reconcile_session_id = sessions.session_id);
```

- Run the `WAYPURGE.GC_SESSIONS dba_job` manually.

```
sqlplus "/ as sysdba"
SQLPLUS> grant create session to gcadmin;
SQLPLUS> connect gcadmin/<password_for_gcadmin>
SQLPLUS> col schema_user format a10
SQLPLUS> col what format a50
SQLPLUS> set line 200
SQLPLUS> select job, schema_user, last_date, this_date, next_date, broken, what from user_jobs where what LIKE
'WAYPURGE%';
```

### Sample output:

```
      JOB SCHEMA_USE LAST_DATE THIS_DATE NEXT_DATE BRO WHAT
-----
      189 GCADMIN 14-APR-10 15-APR-10 N WAYPURGE.GC_SESSIONS;----> note job number

SQLPLUS> exec dbms_job.run(189);
```

Note the time taken by the manual job run and increase the value of `WAY_GC_SESSIONTREES_DELETE_MAX` accordingly. `WAY_GC_SESSIONTREES_DELETE_MAX` value should be gradually increased and the time taken to run the job should be monitored. `WAY_GC_SESSIONTREES_DELETE_MAX` can be increased to say 300, 500, 1000, 3000 and so on.

```
sqlplus "/ as sysdba"
SQLPLUS> grant create session to lcrep;
SQLPLUS> connect lcrep/<password for lcrep>
SQLPLUS> UPDATE audit_params SET value = 1000 WHERE name =
'WAY_GC_SESSIONTREES_DELETE_MAX';
SQLPLUS> commit;
```

Step 2 can be run to monitor the number of records that need to be cleaned up.

- The Waypurge job can be run manually or the nightly `dba_job` can delete the child records. Note that the GC nightly DBA job is run only once a day, so it may take several days for it to delete all the child records. A combination of manual and nightly job run is recommended.

- 4 After all child records are removed, delete the WAY\_GC\_SESSIONTREES\_DELETE\_MAX value from the AUDIT\_PARAMS table.

```
sqlplus "/ as sysdba"
SQLPLUS> grant create session to lcrep;
SQLPLUS> connect lcrep/<password for lcrep>
SQLPLUS> DELETE FROM audit_params WHERE name =
'WAY_GC_SESSIONTREES_DELETE_MAX';
SQLPLUS> Commit;
SQLPLUS> select AUDIT_PARAM_ID, NAME, VALUE from audit_params; ->check that
the value was removed.
```

## Windows Server CLI Installation

If you plan to install the SA Command-line Interface (OCLI) on a Windows Server after upgrade to SA 7.83, you must update the Agent on that server to the latest version. Errors occur during OCLI installation on Windows servers with earlier Agent versions.

## 3 Fixed in SA 7.83

### Fixed in SA 7.83

#### Agents

##### QCCR1D 97923

**Description:** Although the Agent upgrade completes successfully, the Agent Upgrade Custom Extension software returns an unsuccessful upgrade error.

**Platform:** Independent

**Subsystem:** Agent Deployment/Upgrade Backends

**Symptom:** Although the Agent upgrade completes successfully, the Agent Upgrade Custom Extension software returns an unsuccessful upgrade error.

**Resolution:** Fixed

##### QCCR1D 98219

**Description:** When you try to import an exported comma-separated-values (CSV) file, you get the following error:

The following input records were incorrectly formatted and were skipped.

**Platform:** Independent

**Subsystem:** Agent Deployment/User Interface Upgrade

**Symptom:** SA Client cannot import an exported CSV.

**Resolution:** Fixed

##### QCCR1D 102321

**Description:** If you modify the default software policies, during a patch content upload, the Opsware Agent Tools installer returns a missing software policies error instead of updating/creating the missing policy.

**Platform:** Independent

**Subsystem:** Agent Tools

**Symptom:** Opsware Agent Tools installer returns a missing software policies error if you modify the default software policies.

**Resolution:** Fixed

## QCCR1D 103678/108387109467

**Description:** You cannot obtain device manufacturer/hardware information when you issue the `bs_hardware` command. Instead, the software displays the following system diagnostic message:

```
Hardware Stack Shape: Device IDs with unrepresented model_type: [239580100]
```

**Platform:** Windows, Linux, Solaris-x86-64bit

**Subsystem:** Agent

**Symptom:** Instead of displaying device manufacturer/hardware information, the software displays a system diagnostic flag.

**Resolution:** Fixed

## QCCR1D 104974

**Description:** SA Windows agent heartbeat thread starts later than it should.

**Platform:** All Windows

**Subsystem:** Agent

**Symptom:** SA Windows agent heartbeat thread starts later than it should.

**Resolution:** Fixed

## QCCR1D 105363

**Description:** RFE for SA 7.8x support in Chinese locale.

**Platform:** Independent

**Subsystem:** Agent

**Symptom:** SA 7.8x does not currently provide support for Chinese locales.

**Resolution:** Fixed

## QCCR1D 106327

**Description:** Remediation operation fails because of excessive operation output coupled with low caller consumption rates. An unexpected error is returned.

**Platform:** Linux, Solaris

**Subsystem:** Agent

**Symptom:** An unexpected error is returned during a dependency resolution.

**Resolution:** Fixed

## QCCR1D 106621

**Description:** You cannot perform an agent update using the Agent Upgrade tool due to an incompatibility between the tool and the current agent versioning scheme.

**Platform:** Independent

**Subsystem:** Agent Deployment/Upgrade UI

**Symptom:** Under certain circumstances, you cannot perform an agent update using the OPSWopsh tool.



**Resolution:** Fixed

### QCCR1D 106761

**Description:** The software returns an unexpected traceback exception error when you set the Manage Software Policy to Read, and you use the `solpatch_import` command to create a policy.

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

**Symptom:** The software returns an unexpected traceback error when you set the Manage Software Policy to Read.

**Resolution:** Fixed

### QCCR1D 106983

**Description:** When you run a prerequisite installation check for the VMware ESXi server, the Agent performs the check and also begins to manage the server, although the Manage Server menu item is still enabled. The installation check should be disabled.

**Platform:** VMware ESXi

**Subsystem:** Patch Management

**Symptom:** The prerequisite installation check is enabled for VMware ESXi servers, it should be disabled.

**Resolution:** Fixed

### QCCR1D 107706

**Description:** An agent running Python Version 1.5 cannot download a file that is greater than 2 GigaBytes (GB).

**Platform:** HP-UX 11.23, 11.11, and 11.00

**Subsystem:** Agent

**Symptom:** You receive an error when you download depots larger than 2GB.

**Resolution:** Fixed

### QCCR1D 107958

**Description:** Cannot upgrade an agent that is installed on a Windows Server 2008 R2 x86-64.

**Platform:** Windows 2008 R2 x86-64

**Subsystem:** CX - Agent Upgrade

**Symptom:** Cannot upgrade an agent that is installed on a Windows Server 2008 R2 x86-64.

**Resolution:** Fixed

### QCCR1D 108800

**Description:** You cannot close the Unmanaged Servers scanning window by clicking the X icon in the corner.

**Platform:** Independent

**Subsystem:** Agent Deployment/Upgrade UI

**Symptom:** You cannot close the Unmanaged Servers dialog box or the Agent Deployment window by clicking the (X) in the corner.

**Resolution:** Fixed

## QCCR1D 108801

**Description:** You cannot close the Agent Deployment window by clicking the X icon in the corner.

**Platform:** Independent

**Subsystem:** Agent Deployment/Upgrade UI

**Symptom:** You cannot close the Unmanaged Servers dialog box or the Agent Deployment window by clicking the (X) in the corner.

**Resolution:** Fixed

## QCCR1D 109241

**Description:** The Last Deployment Attempt Message in the Summary view is blank.

**Platform:** All Windows

**Subsystem:** Agent Deployment/Upgrade UI

**Symptom:** The Last Deployment Attempt message is blank.

**Resolution:** Fixed

**Subsystem:** Agent Deployment/Upgrade UI

**Symptom:** Agent begins server management unexpectedly on the VMware ESXi server.

**Resolution:** Fixed

## Application Configuration

### QCCR1D 96141

**Description:** Editing errors occur when you create or modify rules in the Application Configuration Audit and Remediation editor.

**Platform:** Independent

**Subsystem:** Application Configuration UI

**Symptom:** Unexpected behaviors (such as duplicate entry creation) are displayed when you create/modify rules in the Application Configuration Audit and Remediation tool.

**Resolution:** Fixed

### QCCR1D 98407

**Description:** When you use the `GroupConfigurable.pushConfiguration()` API call, you receive a null pointer exception.

**Platform:** Independent

**Subsystem:** Application Configuration Backend

**Symptom:** When you use the `GroupConfigurable.pushConfiguration()` API call, you receive a null pointer exception.

**Resolution:** Fixed

## QCCR1D 102551

**Description:** In the Application Configuration Audit and Remediation tool, an entire rule is remediated if a part of that rule fails, but only the failed part should be remediated.

**Platform:** Independent

**Subsystem:** Application Configuration CML Engine

**Symptom:** When part of a rule fails, the entire rule is remediated.

**Resolution:** Fixed

## QCCR1D 105927

**Description:** The Application Configuration tool copies files to the target location instead of moving them, causing some applications to return an error when they read a 0-byte configuration file.

**Platform:** Independent

**Subsystem:** Application Configuration Backend

**Symptom:** Some applications return an error when they read 0-byte configuration files.

**Resolution:** Fixed

## QCCR1D 106965

**Description:** For partial templates, the Preserve Format menu option in the Application Defaults valueset editor only has the Yes value enabled. However, when you choose this option and save it, its value resets to a blank value.

**Platform:** Independent

**Subsystem:** Application Configuration User Interface

**Symptom:** For partial templates, the Preserve Format option limits the values you can set and automatically defaults to a blank value.

**Resolution:** Fixed

## Audit and Compliance

### QCCR1D 107794

**Description:** When you create hundreds of Register Software rules at a time during an audit, the run dialog and the audit log file display an out-of-memory (OOM) error.

**Platform:** Independent

**Subsystem:** Audit and Compliance user interface

**Symptom:** The graphical user interface (GUI) and the audit log file display an OOM error during an audit.

**Resolution:** Fixed

## QCCR1D 108376

**Description:** The HTTP server waits a few seconds before disconnecting after it has read remote configuration files. When you conduct configuration scans against a large number of servers (60 or more) with 60 or more managed configuration files, this HTTP-server behavior produces too many MAXIMUM timeouts on the individual scanned servers.

**Platform:** Independent

**Subsystem:** Audit and Compliance - Backend

**Symptom:** HTTP server disconnection lags cause a large number of MAXIMUM timeouts on the individual scanned servers.

**Resolution:** Fixed

## QCCR1D 108454

**Description:** The graphical user interface in the SA Client freezes when you try to download a large audit result. After a longer than usual time, an audit result browser eventually displays the result.

**Platform:** Independent

**Subsystem:** Audit and Compliance - UI

**Symptom:** The graphical user interface in the SA Client freezes when you try to download a large audit result.

**Resolution:** Fixed

## QCCR1D 110370

**Description:** Audit snapshot files are too large and take up too much storage room.

**Platform:** Independent

**Subsystem:** Audit and Compliance - Backend

**Symptom:** Snapshots files generated when you run multiple audit Register Software rules become very large and take up a lot of storage space.

**Resolution:** Fixed

## QCCR1D 110871

**Description:** Audit custom scripts either time out without producing a result (such as when the script is waiting for an input command) or enter an endless loops. Some compliance checks whose parameters have not been set experience the same phenomenon.

**Platform:** Independent

**Subsystem:** Audit and Compliance - Backend

**Symptom:** Custom scripts either time out without producing a result or enter an endless loop.

**Resolution:** Fixed

## Automation Platform Extensions (APX)

### QCCR1D 105597

**Description:** An Automation Platform Extensions (APX) Program fails to run (from either a group or an All Managed Servers list) after you press the Start Job button in the last step.

**Platform:** Independent

**Subsystem:** APX - Web Application

**Symptom:** Pressing the Start Job button in the last step of an Extensible Discovery APX Program run does not start the application.

**Resolution:** Fixed

## Command Center

### QCCR1D 107732

**Description:** You cannot create search criteria based on virtualization because the search text field gathers characters in reverse order.

**Platform:** Independent

**Subsystem:** OCC Client Framework

**Symptom:** Virtualization searches are invalid due to search-text field error.

**Resolution:** Fixed

## Command Engine

### QCCR1D 98445

**Description:** When you choose Tools ► Options in the SA Client, the cursor becomes unresponsive.

**Platform:** Independent

**Subsystem:** OCC Client Framework

**Symptom:** When you choose Tools ► Options in the OO Client, the cursor becomes unresponsive.

**Resolution:** Fixed

### QCCR1D 102616

**Description:** Environment variables in scripts do not always resolve as expected.

**Platform:** All Unix (AIX, HP-UX, Solaris, Linux)

**Subsystem:** Command Engine - Way

**Symptom:** Environment variables in scripts do not always resolve as expected.

**Resolution:** Fixed

With this fix the environment for UNIX will be the following:

- HOME: users home directory (new in 7.8.03)

- LOGNAME: users login name (new in 7.8.03)
- USER: same as LOGNAME (new in 7.8.03)
- TZ: time zone (not supported on Linux)
- PATH: (modified in 7.8.03 - see below)
- SHELL: /usr/bin/sh (/usr/bin/ksh on AIX /bin/sh for Linux)
- TERM: dumb
- HOSTTYPE: i386 (Linux only)
- SHLVL: 2 (Linux only)
- OSTYPE: Linux (Linux only)
- LANG: C (AIX, HP-UX)
- ODMDIR: /etc/objrepos (AIX only)
- LC\_\_FASTMSG: true (AIX only)

The values of PATH are as follows:

- Solaris: /bin:/usr/bin:/usr/sbin
- Solaris (root): /sbin:/bin:/usr/sbin:/usr/bin
- Linux: /usr/local/bin:/bin:/usr/bin
- Linux (root): /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
- AIX: /usr/bin:/usr/sbin
- AIX (root): /sbin:/bin:/usr/sbin:/usr/bin
- HP-UX: /usr/bin:/bin:/sbin:/usr/sbin
- HP-UX (root): /sbin:/bin:/usr/sbin:/usr/bin

The value of SHELL will always be set to /usr/bin/sh except on AIX and Linux. The sh script is always executed in sh (not bash or any other shell). Other shells or runtimes can be executed by adding a #! <path> at the top of the sh script.

Customers who want to have their .profile (or any other script) executed must explicitly do so in the sh script.

## Custom Extensions

### QCCR1D 108148

**Description:** There are no custom user-interface extensions (such as Change Password CX) that effect changes to the server in the Approval Integration engine.

**Platform:** Independent

**Subsystem:** Custom Extensions

**Symptom:** The Approval Integration engine does not have custom extensions that affect the server.

**Resolution:** Fixed - Added approval integration to custom extensions. In the SA Web Client, the new jobs will be listed as Run Custom Extensions and the old jobs as Run Custom Extension. This does not change previously run or scheduled jobs, only jobs created after the 7.83 patch is applied.

## DCML Tool (DET)

### QCCR1D 107377

**Description:** Recurrence of bug with DCML (DET) command line utility.

**Platform:** Linux

**Subsystem:** DCML Export Tool (DET)

**Symptom:** The CBT Import does not correctly restore command options of an Install/Uninstall Sequence Policy Item script. Instead, the import sets the same Command Options for both the install and uninstall sequences.

**Resolution:** Fixed

In order for this issue to be completely addressed, both the importing core and exporting core must be, at minimum:

**Table 6** Minimum Version Level

Exporting Core	Importing Core
7.50.07	7.50.07
7.50.07	7.83
7.83	7.83

## Global File System

### QCCR1D 107483

**Description:** Users are not deleted from the user cache. Subsequently, those same users cannot access the OGFS because the system considers them re-created users.

**Platform:** Independent

**Subsystem:** Global Filesystem/Shell Backend

**Symptom:** Users are not deleted from the Global File System user cache.

**Resolution:** Fixed

### QCCR1D 109315

**Description:** Global File System produces an OutOfMemoryError (OOM) during a larger audit.

**Platform:** Independent

**Subsystem:** Global File System

**Symptom:** An audit fails with an OOM error during a larger audit.

**Resolution:** Fixed

## Model Repository

### QCCR1D 108378

**Description:** The Compliance Dashboard takes a long time to load, resulting in a high CPU load on the database server.

**Platform:** Independent

**Subsystem:** Model Repository

**Symptom:** Compliance Dashboard load time results in high CPU load.

**Resolution:** Fixed

## OS Provisioning

### QCCR1D 93355

**Description:** When you use the `import_media` command to update an operating system installation media name that is already imported, the media name is not updated in the SAS Web Client.

**Platform:** Independent

**Subsystem:** OS Provisioning - Backend

**Symptom:** Media name is not updated in the SAS Web Client when you update the operating system installation media.

**Resolution:** Fixed

### QCCR1D 106181

**Description:** When you select an operating system installation profile in the SAS Web Client, the WinPE attributes are not displayed.

**Platform:** Windows

**Subsystem:** OS Provisioning - SAS Web Client

**Symptom:** When you select an operating system installation profile in the SAS Web Client, the WinPE attributes are not displayed.

**Resolution:** Fixed

### QCCR1D 107291

**Description:** Customer Request: WinPE HP iLO from SSTK driver request for HP DL 380 G6.

**Platform:** Independent

**Subsystem:** OS Provisioning Backend

**Symptom:** HP iLO driver from the SmartStart Scripting Toolkit should be included in the WIMs.

**Resolution:** Fixed



## QCCR1D 108110

**Description:** If you run an Install Sequence job, scrolling is disabled in the Select Server and Preview Steps results.

**Platform:** Independent

**Subsystem:** OS Provisioning - SA Command Center - client

**Symptom:** If you run an Install Sequence job, scrolling is disabled in the Select Server and Preview Steps results.

**Resolution:** Fixed

## QCCR1D 108111

**Description:** When you run an operating system sequence job, detail panes of selected servers displayed in an active job window close unexpectedly and are difficult to reopen.

**Platform:** Independent

**Subsystem:** OS Provisioning - OCC - client

**Symptom:** Detail panes of selected servers displayed in an active job window close unexpectedly and are difficult to reopen.

**Resolution:** Fixed

## QCCR1D 108113

**Description:** When you run an Install Sequence job, you cannot sort in the resulting job-window table.

**Platform:** Independent

**Subsystem:** OS Provisioning - SA Command Center - client

**Symptom:** When you run an Install Sequence job, you cannot sort in the resulting job-window table.

**Resolution:** Fixed

## QCCR1D 109393

**Description:** For HP iLO firmware versions 1.78 and 1.79, the Manage Boot Clients (MBC) for the server with HP iLO secure socket layer connections throws connection timeout errors when it retrieves details from the iLO interface.

**Platform:** Independent

**Subsystem:** OS Provisioning - Backend

**Symptom:** The MBC throws connection timeout errors when retrieving details from the iLO interface.

**Resolution:** Fixed

## Patch Management - Solaris

### QCCR1D 102564

**Description:** When you attempt to do an attach and remediate operation without first running the `create_db` script on the core, the software compliance scan status displays a `Scan failed` error.

**Platform:** Solaris 5.10, 5.10 x86, 5.9, 5.8, 5.7, 5.6

**Subsystem:** Patch Management - Solaris Server

**Symptom:** During an attach and remediate operation, you see a `Scan failed` error in the software compliance scan-status field.

**Resolution:** Fixed

### QCCR1D 105981

**Description:** When remediating a Solaris patch bundle or a Solaris cluster, the value of the `way.remediate.action_timeout` parameter should be set to the highest value of the three values in the following parameters: `way.remediate.solaris_cluster_package_alarm_timeout`, `way.remediate.action_timeout`, and `way.remediate.package_alarm_timeout`. If the value of the `way.remediate.action_timeout` parameter is less than the value of the `solaris_cluster_package_timeout`, the `way.remediate.action_timeout` expires first, causing the job to time out.

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

**Symptom:** If the value of the `way.remediate.action_timeout` is less than the value for the `solaris_cluster_package_timeout`, the `way.remediate.action_timeout` would expire first, causing the job to time out.

**Resolution:** Fixed

### QCCR1D 107130

**Description:** After a new server is assimilated into the core, the applicability calculation incorrectly reports that bundles are non-applicable to the server, despite the fact that there is no software-registration data.

**Platform:** Solaris 5.10, 5.10 x86, 5.9, 5.8, 5.7, 5.6

**Subsystem:** Patch Management - Solaris

**Symptom:** Incorrect applicability calculation reports that bundles are not applicable.

**Resolution:** Fixed

### QCCR1D 108503

**Description:** For Solaris 7.82/7.81 patches that are not yet imported, the user interface freezes when you click the Vendor Documentation link in the patch browser.

**Platform:** Solaris 5.10, 5.10 x86, 5.9, 5.8, 5.7, 5.6

**Subsystem:** Patch Management - Solaris

**Symptom:** User interface freezes when you click the Vendor Documentation link in the patch browser.

**Resolution:** Fixed

## Patch Management - Unix

### QCCR1D 107109

**Description:** During patch remediation, some AIX packages fail and display the following error:

```
ValueError: invalid literal for int(): v>3
```

**Platform:** AIX

**Subsystem:** Patch Management - Unix

**Symptom:** During patch remediation, some AIX packages fail and display invalid literal errors.

**Resolution:** Fixed

### QCCR1D 108222

**Description:** Some notes do not display in the job-status details of the SA output display when you install two patches and one patch supersedes the other.

**Platform:** HP-UX

**Subsystem:** Patch Management - Unix - UI

**Symptom:** Not all notes display in the SA output display.

**Resolution:** Fixed

## Patch Management - Windows

### QCCR1D 107897

**Description:** Windows agents fail to report installed BSA Essentials Network (BSAEN) patches that have software releases in the form: /packages/any/nt/.

**Platform:** All Windows

**Subsystem:** Patch Management - Windows - Backend

**Symptom:** Windows agents fail to report installed and recommended BSAEN patches.

**Resolution:** Fixed

## SA Client

### QCCR1D 109052

**Description:** You cannot add a device group to a User group's access-control list if the device group has the same name as an existing user for that User group.

**Platform:** Independent

**Subsystem:** Server Groups UI

**Symptom:** You cannot add a device group to a User group's access-control list if the device group has the same name as an existing user for that User group.

**Resolution:** Fixed

## SA Installer

### QCCR1D 105675

**Description:** After a rollback from SA 7.82 to 7.80, the SA version is shown incorrectly. It still shows as 7.82 instead of 7.80.

**Platform:** Independent

**Subsystem:** SA Installer

**Symptom:** SA version is not updated after a rollback is applied.

**Resolution:** Fixed

## Search

### QCCR1D 110005

**Description:** Advanced searches failed to display a list of windows services for Windows 64-bit operating systems.

**Platform:** Windows Server 2008 x86-64, Windows Server 2003 x86-64

**Subsystem:** Search

**Symptom:** Advanced search failed to display a list of windows services for Windows 64-bit operating systems.

**Resolution:** Fixed

## Server Management - Managed Servers

### QCCR1D 80776

**Description:** The Network Association box in the device group properties page appears unchecked even if the group is already associated to a network.

**Platform:** Independent

**Subsystem:** Server Management - Managed Servers

**Symptom:** The Network Association box in the device group properties page appears unchecked even if the group is already associated to a network.

**Resolution:** Fixed

### QCCR1D 107142

**Description:** You cannot change the value of the Server Use or Server Stage fields in the SA Client.

**Platform:** Independent

**Subsystem:** Server Management - Managed Servers

**Symptom:** You cannot change the value of the Server Use or Server Stage fields in the SA Client.

**Resolution:** Fixed

## QCCR1D 108074

**Description:** After you use the Manage Boot Clients (MBC) to set server stage and use fields, the SA Client displays inconsistent field information, but the SAS Web Client and the OGFS display the correct information.

**Platform:** Independent

**Subsystem:** Server Management - Managed Servers

**Symptom:** The SA Client displays inconsistent field information.

**Resolution:** Fixed

## Server Module (SMO)

### QCCR1D 101980

**Description:** If you scan a server for its runtime state, the software throws an exception and does not return any information.

**Platform:** Linux

**Subsystem:** Server Module

**Symptom:** If you scan a server for its runtime state, the software throws an exception and does not return any information.

**Resolution:** Fixed

### QCCR1D 105810

**Description:** When you perform a runtime state scan of a server, it does not display the existing logged-in users.

**Platform:** CentOS 5

**Subsystem:** Server Module

**Symptom:** Logged-in users are not displayed during a runtime state scan of the server.

**Resolution:** Fixed

## Software Management

### QCCR1D 99631

**Description:** You cannot force a server to reboot during a software remediation if the Suppress Reboot option is enabled.

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)

**Symptom:** You cannot force the machine to reboot during a software remediation.

**Resolution:** Fixed

## QCCR1D 102471

**Description:** The server clock and the core clock are not synchronized, so reported remediation times can be inconsistent because some devices use the server clock and some the core clock.

**Platform:** Independent

**Subsystem:** Software Management - API - Package

**Symptom:** The server clock and the core clock are not synchronized.

**Resolution:** Fixed

## QCCR1D 106606

**Description:** The `import_aix_packages` utility does not always properly detect patch files.

**Platform:** AIX

**Subsystem:** Software Management - Tools

**Symptom:** The `import_aix_packages` utility does not always properly detect patch files.

**Resolution:** Fixed

## QCCR1D 106847

**Description:** You receive an endless Invalid LPP file error when you try to import an AIX patch bundle.

**Platform:** AIX

**Subsystem:** Software Management - Tools

**Symptom:** Endless Invalid LPP file error is displayed when you try to import an AIX patch bundle.

**Resolution:** Fixed

## QCCR1D 107877

**Description:** The `yum` wrapper fails to treat the `kernel-default-base` script as an install-only package.

**Platform:** SuSE 11

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

**Symptom:** The `yum` wrapper fails to treat the `kernel-default-base` script as an install-only package.

**Resolution:** Fixed

## QCCR1D 108442

**Description:** The Solaris package handler does not search the full custom attribute scope when it looks for the `SolarisAdminFile` custom attribute because the file is not attached to a device.

**Platform:** Solaris

**Subsystem:** Software Management - Backend - Remediate (Other)

**Symptom:** The `SolarisAdminFile` custom attribute is not honored when it is not attached to a device.

**Resolution:** Fixed

## QCCR1D 108776

**Description:** When Python-based daemons run out of file descriptors, they stop serving requests because 32-bit programs that use standard input/output are limited to 256 file descriptors.

**Platform:** Solaris

**Subsystem:** Data Access Engine

**Symptom:** Python-based daemons run out of file descriptors and stop serving requests.

**Resolution:** Fixed

## QCCR1D 109818

**Description:** If you select the `Hold reboots until the end` option, and then echo `OPSW_REBOOT` from a script in a software policy, the managed server does not reboot.

**Platform:** Windows

**Subsystem:** Software Management

**Symptom:** Echoing `OPSW_REBOOT` in a script does not reboot the server.

**Resolution:** Fixed

## QCCR1D 110199

**Description:** The remediate servers operation (`ServerService.startFullRemediateNow()`) in the SA WebServices/Data Access Engine does not work. There is no device identifier for the job, so the remediate operation to the agent does not occur.

**Platform:** All Windows

**Subsystem:** Software Management - API - Software Policy

**Symptom:** The remediate servers operation (`ServerService.startFullRemediateNow()`) in the SA WebServices/Data Access Engine does not work.

**Resolution:** Fixed

## Web Services Data Access Engine

### QCCR1D 105241

**Description:** The `AuthorizationService.findAuthorizedResources()` API call/authorization service fails for the `OperationConstants.READ_USER` operation, resulting in an Oracle error.

**Platform:** Independent

**Subsystem:** Web Services Data Access Engine

**Symptom:** Under certain circumstances, the SA authorization service results in an Oracle Error.

**Resolution:** Fixed

### QCCR1D 107878

**Description:** Import/Export packages time out in the SA Client if there is no direct access to port 443 of the Core Gateway.

**Platform:** Independent

**Subsystem:** Web Services Data Access Engine

**Symptom:** Import/export packages time out in the SA Client.

**Resolution:** Fixed

## QCCR1D 109256

**Description:** Linking to RHEL audit policy throws ORA-01795: maximum number of expressions in a list is 1000

**Platform:** Linux

**Subsystem:** Web Services Data Access Engine

**Symptom:** Importing an audit policy populates the audit with all rules for the imported policy. Changing the policy requires you to delete all the old rules. As there are more than 1000 rules in the audit policy, ORA-01796 occurs when using the DELETE operation.

**Resolution:** Fixed

## QCCR1D 109318

**Description:** Audit jobs and snapshots of most of the servers are completed, but the results are not available. The audit results calculations are aborted with Oracle error: ORA-00060: deadlock detected while waiting for resource.

**Platform:** Linux Solaris

**Subsystem:** Web Services Data Access Engine

**Symptom:** Oracle deadlock errors are displayed during audit results calculations.

**Resolution:** Fixed

## QCCR1D 110459

**Description:** You might experience performance issues in the dynamic-device group membership calculation if you run a large number of servers.

**Platform:** Independent

**Subsystem:** Web Services Data Access Engine

**Symptom:** You might experience performance issues in the dynamic-device group membership calculation if you run a large number of servers.

**Resolution:** Fixed

## QCCR1D 110988

**Description:** Inefficient SQL inline views cause the Selector Manager to return SQL queries with a longer execution time than normal.

**Platform:** Independent

**Subsystem:** Web Services Data Access Engine



**Symptom:** Inefficient SQL inline views cause the Selector Manager to return SQL queries with a longer execution time than normal.

**Resolution:** Fixed

## Fixed in SA 7.82

### Agents

#### QCCR1D 98761

**Description:** If an LPP fileset is generated with a type other than “F” (fileset), for example (MF), SA installs the fileset but cannot recognize it once installed.

**Platform:** AIX

**Subsystem:** Agents

**Symptom:** If an LPP fileset is generated with a type other than “F” (fileset), for example (MF), SA installs the fileset but cannot recognize it once installed.

**Resolution:** Fixed

#### QCCR1D 101916

**Description:** SA 7.80 Agent memory faults occur on AIX servers that have ethernet aliases configured.

**Platform:** AIX

**Subsystem:** Agents

**Symptom:** No interfaces reported on AIX servers with configured ethernet aliases.

**Resolution:** Fixed

#### QCCR1D 102457

**Description:** SA should support installing packages in an alternate target root path as Solaris `pkgadd` can using the `-R` argument.

**Platform:** Solaris

**Subsystem:** Agents

**Symptom:** SA does not support installation of Solaris packages to an alternate root path.

**Resolution:** Fixed

#### QCCR1D 103666

**Description:** A route index entry for an interface not found in the device map causes `bs_hardware` to fail.

**Platform:** Windows

**Subsystem:** Agents

**Symptom:** When running `bs_hardware.bat`, you see an error similar to:

```
'errors': {'interfaces': [['Traceback (most recent call last):\n',\n' File ".\\nt\\nt_network\\nt_interface.py", line 347, in readConfig\n',\n' File ".\\nt\\nt_network\\nt_interface.py", line 371, in\ngetPrimaryInterfaceName\n',\n'KeyError: 1\n']]]},
```

in the output.

You may also notice that information about one or more network adapters is not updated correctly in the core.

**Resolution:** Fixed

## QCCR1D 103702

**Description:** In Solaris 10 U8 **Inventory** ► **Storage** ► **Disks** panel, Local Disks are not shown.

**Platform:** Solaris

**Subsystem:** Agents

**Symptom:** Local Disks are not shown in **Inventory** ► **Storage** ► **Disks** panel.

**Resolution:** Fixed

## QCCR1D 104589

**Description:** On HP-UX managed servers, the TZ variable is not picked up correctly from default system configuration files.

**Platform:** HP-UX

**Subsystem:** Agent

**Symptom:** The time zone environment variable is not set properly on HP-UX agents.

**Resolution:** Fixed

## Audit and Compliance

### QCCR1D 102870

**Description:** The standard output from custom script rules should be persisted to the Model Repository so that the data can be included in compliance reports.

**Platform:** Independent

**Subsystem:** Audit & Compliance Backend

**Symptom:** The standard output from pluggable checks is not transferred from the SA Model Repository to OMDB for reporting purposes.

**Resolution:** Fixed

## Automation Platform Extensions (APX)

### QCCR1D 82077

**Description:** The `apxtool new` command creates a source directory before user confirms directory creation.

**Platform:** Independent

**Subsystem:** APX tool

**Symptom:** Although the user is prompted to confirm the creation of the source directory, the `apxtool new` command creates the directory regardless of the user confirmation.

**Resolution:** Fixed

### QCCR1D 91006

**Description:** Should provide the ability to mark an APX as excluded in Approval Integration.

**Platform:** Independent

**Subsystem:** APX - Other

**Symptom:** Approval Integration behavior does not currently allow APXs (such as a control APX) to be run when Approval Integration is enabled for APXs. User should be able to exclude specified APXs from Approval Integration

**Resolution:** Fixed

### QCCR1D 91231

**Description:** MBC DHCP Cleanup APX dumps traceback errors if the `dhcpd.conf` file does not exist.

**Platform:** Independent

**Subsystem:** APX - Other

**Symptom:** When the DHCPd configuration file `/etc/opt/opsware/dhcpd/dhcpd.conf` is not present on the core server, the MBC APX `dhcp_cleanup_apx` dumps traceback errors. In SA 7.82 and later, if the `dhcp.conf` file is not present the following error will be displayed:

```
Error: The DHCP config file '/etc/opt/opsware/dhcpd/dhcpd.conf' does not exist on this core.  
Skipping restart of dhcpd.
```

**Resolution:** Fixed

### QCCR1D 97914

**Description:** Should be able to right-click on an APX to run it when in the Device Group view.

**Platform:** Independent

**Subsystem:** APX - WebApp

**Symptom:** In the Device Groups view, there is no `Run Extension` option.

**Resolution:** Fixed

## QCCR1D 100912

**Description:** `apxtool` should populate `apx.cfg` with "folder name" if the user provides one when creating a new APX.

**Platform:** Independent

**Subsystem:** APX tool

**Symptom:** When a new APX description is created using the `apxtool new` command, the `apx.cfg` generated by the tool does not contain a property "folder\_path" even if the folder was specified on the command line by the user. As a result the following import command will not have enough information to upload the APX to the core.

**Resolution:** Fixed

## QCCR1D 103757

**Description:** When running the Manage Boot Clients (MBC) utility with large amounts of data, it sometimes throws an error when trying to read/interpret the progress file.

**Platform:** Independent

**Subsystem:** APX - WebApp

**Symptom:** When running MBC with large amounts of data, it sometimes throws an error when trying to read/interpret the progress file.

**Resolution:** Fixed

## QCCR1D 103836

**Description:** The APX Tool doesn't allow non-interactive execution when the `USER` variable is not present, even for root.

**Platform:** Solaris

**Subsystem:** APX tool

**Symptom:** In some cases it is not possible to run the APX Tool without being prompted for your username/password. This interfere with such non-interactive processes as patching the core.

**Resolution:** Fixed

## QCCR1D 106153

**Description:** User specified folders are ignored when creating a description for a new APX using the APX Tool.

**Platform:** Independent

**Subsystem:** APX tool

**Symptom:** When a user creates a description for a new APX using the APX Tool to specify the folder, the folder is not created. Instead, the description is placed in the default folder. For example:

```
apxtool new -t script -u com.opsware.apx.program -d ApxProgramTest src -F
```

After execution of the command above, the expected folder `src` is not created. Instead, the `com.opsware.apx.program` folder is created and the APX is loaded into it.

**Resolution:** Fixed

## Command Engine

### QCCR1D 97400

**Description:** The Global Shell window can terminate when selecting **Action ► Run** to launch an OGFS script.

**Platform:** Linux/Solaris

**Subsystem:** OCC Client Framework

**Symptom:** Global Shell window terminates when launching an OGFS script.

**Resolution:** Fixed

### QCCR1D 102836

**Description:** Cannot launch SA Client under Microsoft Windows 7.

**Platform:** Windows 7

**Subsystem:** OCC Client Framework

**Symptom:** Running the SA Client launcher under Windows 7 fails (no login dialog appears).

**Resolution:** Fixed

### QCCR1D 103175

**Description:** Dragging and dropping files does not support multi-selection copying for managed servers.

**Platform:** Windows

**Subsystem:** OCC Client Framework

**Symptoms:**

1. The user can select group of files and she/he drag them, but only one of the files is copied.
2. If the first selected object is a folder, then moving a mouse just changes the selection in the pane. If the first item is a file, then that file will be drag-n-dropped.

**Resolution:** Fixed

### QCCR1D 103955

**Description:** Cannot create an SA username that consists only of numbers.

**Platform:** Independent

**Subsystem:** OCC Web - Administration

**Symptom:** SA doe not allow user creation unless the name begins with an alpha character (a-zA-Z]).

**Resolution:** Fixed

## Data Access Engine

### QCCR1D 102962

**Description:** SA does not detect the operating system of a Windows Server 2008 managed server that has been upgraded to R2.

**Platform:** Windows 2008

**Subsystem:** Data Access Engine (spin)

**Symptom:** Win2008 R2 servers are shown in the SA Client with platform Unknown.

**Resolution:** Fixed

## DCML Tool (DET)

### QCCR1D 101734

**Description:** Audit Compliance Checks can not be deprecated with cbt tool during import.

**Platform:** Independent

**Subsystem:** DCML Export Tool (DET)

**Symptom:** Audit Compliance Checks can not be deprecated with cbt tool during import.

**Resolution:** Fixed

## Distributed Scripts

### QCCR1D 82714

**Description:** After running a distributed script, exporting job output to a report is limited to 10K. Users should be able to adjust output size.

**Platform:** Linux, Solaris, Windows

**Subsystem:** Distributed Scripts (DSE) (UI)

**Symptom:** Exporting the results of job output to a report from the Run Script dialog is limited to 10K. Therefore, job output is truncated.

**Resolution:** Fixed

## Extensible Discovery

### QCCR1D 102187

**Description:** SA should support a single script that reports multiple attributes/values for Extensible Discovery.

**Platform:** Independent

**Subsystem:** Extensible Discovery

**Symptom:** When using Extensible Discovery to discovery attributes about multiple instances you must pre-define the exact list of attributes to be discovered and stored - creating a separate script for each attribute. SA should support a single script that reports multiple attributes/values.

**Resolution:** Fixed

## Global File System

### QCCR1D 92767

**Description:** An OGFS IO Error occurs on Windows Servers with character set specified as CP936.

**Platform:** Linux/Solaris

**Subsystem:** Global Filesystem/Shell Backend

**Symptom:** Accessing Windows managed server with character set specified as CP936 in the OGFS environment results in I/O error.

**Resolution:** Fixed

## Installer

### QCCR1D 100931

**Description:** A rollback from SA 7.81 to 7.80 reports the error: Failed to remove software policy 'Storage Compliance Checks' (8710001)

**Platform:** Independent

**Subsystem:** Installer

**Symptom:** During rollback from SA 7.81 to 7.80, an error is reported in the console and stored in the correspondent log-file under /var/log/opsware/opsware\_installer:

```
Removing com.opsware.server.module.storage.compliance
This will probably take a long time.
```

```
...
```

```
Failed to remove ServerModule from servers
```

```
Traceback (most recent call last):
```

```
File "src/smtool/ServerModule.py", line 352, in remediateSoftwarePolicy
```

```
.....
```

```
File "./asyncssl.py", line 390, in _raw_recv
```

```
error: (104, 'Connection reset by peer')
```

```
Failed to remove software policy 'Storage Compliance Checks' (8710001)
```

```
ProtocolError: <ProtocolError for 192.168.161.22/cogrpc.py: 404 Not found>
```

Rollback fails to remove Storage Compliance. After reporting the error, the rollback continues to the next component and successfully completes.

**Resolution:** Fixed

### QCCR1D 101197

**Description:** While patching an SA 7.80 Core, the installer reports an error: Exception: ERROR: There is no role by the name "Opware System Administrators."

**Platform:** Independent

**Subsystem:** Installer

**Symptom:** While patching a 7.8 core the installer reports the following error:

Traceback (most recent call last):

```
File "./oi_patch_scripts/QC96315.py", line 253, in ?
File "./oi_patch_scripts/QC96315.py", line 241, in main
File "./oi_patch_scripts/patchQC.py", line 61, in apply
File "./oi_patch_scripts/QC96315.py", line 46, in doApply
File "./oi_patch_scripts/QC96315.py", line 169, in setPermissions
File "./oi_patch_scripts/QC96315.py", line 163, in getAAARoleId
Exception: ERROR: There is no role by the name "Opware System Administrators"
```

However the installer handles that unexpected situations and successfully patches the core.

**Resolution:** Fixed

## QCCR1D 106279

**Description:** Software repository installation fails with OptimisticConcurrencyException error.

**Platform:** Linux

**Subsystem:** Installer

**Symptom:** Software repository installation fails with OptimisticConcurrencyException error.

**Resolution:** Fixed

## OS Provisioning

### QCCR1D 82514

**Description:** The Manage Boot Clients (MBC) utility's facility dropdown box uses the display name, but the DHCPD Cleanup facility dropdown uses the short name.

**Platform:** Independent

**Subsystem:** OS Provisioning - OCC - client

**Symptom:** In the MBC General Form, the Facility Dropdown box shows the Facility Display name. However in the DHCPD Cleanup tool, the Facility dropdown box shows the Facility Short name

**Resolution:** Fixed

### QCCR1D 92597

**Description:** OS Provisioning VMWare ESX 3.5 U4 fails with a timeout due to firewall issues.

**Platform:** VMWare ESX 3.5 Update 4

**Subsystem:** OS Provisioning Backend

**Symptom:** Near the end of the OS Provisioning process for VMWare ESX 3.5 U4, the job will fail with the following error:

```
FAILED: Retry transition timed out
```

**Resolution:** Fixed



## QCCR1D 96317

**Description:** Manage Boot Clients (MBC) iLO: Server power on fails if the MAC address that belongs to a PCI/Mezzanine NIC is used instead of the built-in Server NIC.

**Platform:** All Cores with HP iLO interfaces

**Subsystem:** OS Provisioning Backend

**Symptom:** When using a PCI/Mezzanine network card, the server fails to be powered on via HP iLO with an error similar to the following:

```
Updated 1 Cust Attrs. The MAC address specified (XX-XX-XX-XX-XX-XX) doesn't
match any of the ones reported by iLO
(XX-XX-XX-XX-XX-XX,XX-XX-XX-XX-XX-XX,XX-XX-XX-XX-XX-XX,XX-XX-XX-XX-X
X-XX-XX,XX-XX-XX-XX-XX-XX), skipping iLO actions.
```

**Resolution:** Fixed

## QCCR1D 96408

**Description:** Performing OS Provisioning using the Manage Boot Clients (MBC) utility on Linux servers with multiple NICs can result in multiple server records.

**Platform:** Linux

**Subsystem:** OS Provisioning Backend

**Symptom:** On servers that have multiple NICs, using the Managed Boot Client (MBC) utility to perform OS provisioning can result in two server records for the same server if the MAC address specified in MBC is different from the MAC address of the PXE-booted network card.

**Resolution:** Fixed

## QCCR1D 97493

**Description:** WinPE-based OS provisioning can fail when editing WinPE build scripts to specify a domain, username, and password for the Windows OS Media (Samba) server.

**Platform:** Windows

**Subsystem:** OS Provisioning Backend

**Symptom:** WinPE-based OS provisioning can fail when editing WinPE build scripts to specify a domain, username, and password for the Windows OS Media (Samba) server.

**Resolution:** Fixed

## QCCR1D 98240

**Description:** The Manage Boot Clients (MBC) utility takes longer than it should when given a large number of server records to create.

**Platform:** Independent

**Subsystem:** OS Provisioning

**Symptom:** MBC Web APX times out when it must create a large number of server records.

A timeout parameter has been introduced in Multiple Client CSV form that you can use to enter a reasonable timeout value. The default value is 30 minutes.

**Resolution:** Fixed

## QCCR1D 99477

**Description:** The character set in the Manage Boot Clients (MBC) HTML should be set to `utf8`, instead of `iso-8859-1`.

**Platform:** Independent

**Subsystem:** OS Provisioning - OCC - client

**Symptom:** MBC Web APXs use the character set `iso-8859-1`. This should be changed to `utf-8` so that foreign characters are decoded correctly.

**Resolution:** Fixed

## QCCR1D 99976

**Description:** HP RAID controller configuration fails for linux5-based PXE boot with an error.

**Platform:** Linux

**Subsystem:** OS Provisioning Backend

**Symptom:** HP RAID controller configuration fails for linux5-based PXE-boot with the error:

`This version of linux is not supported`

**Resolution:** Fixed

## QCCR1D 100476

**Description:** The Manage Boot Clients (MBC) utility should handle lack of write access to server records more gracefully.

**Platform:** Independent

**Subsystem:** OS Provisioning Backend

**Symptom:** If an SA user lacks write access to server records (due to lack of `read+write` access on customers to which those servers belong), the MBC program APX outputs traceback errors.

**Resolution:** Fixed

## QCCR1D 102332

**Description:** The Manage Boot Clients (MBC) utility can assign a server to a customer that the user does not have write access to.

**Platform:** Independent

**Subsystem:** OS Provisioning Backend

**Symptom:** When a user has Read Only access to a customer and MBC is run with a server record with the `customer=Read Only`, it creates the server record and assigns it to the Read-Only customer.

**Resolution:** Fixed

## QCCR1D 102341

**Description:** The Manage Boot Clients (MBC) utility web APX may fail to read the progress file when it is processing a large number of servers.

**Platform:** Independent

**Subsystem:** OS Provisioning Backend

**Symptom:** When running MBC with large amounts of data, it can throw an error when trying to read/interpret the progress file.

**Resolution:** Fixed

## QCCR1D 102449

**Description:** When provisioning Windows 2008 R2 VL, the value specified for the ProductKey custom attribute is not passed correctly and causes the provisioning to stall with an invalid key error.

**Platform:** Windows 2008 R2

**Subsystem:** OS Provisioning Backend

**Symptom:** OS Provisioning jobs will fail, if the user is relying on Custom Attribute substitution of the ProductKey element of the unattend.xml.

**Resolution:** Fixed

## QCCR1D 102830

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

**Platform:** Independent

**Subsystem:** OS Provisioning - OCC - Client

**Symptom:** The timeout value field in the OS Sequence dialog was overlaid by another field, so there was no way to enter a timeout value.

**Resolution:** Fixed

## QCCR1D 103911

**Description:** OS Provisioning should support HP Nitrogen blade servers equipped with Emulex cards.

**Platform:** Independent

**Subsystem:** OS Provisioning Backend

**Symptom:** OS Provisioning fails on HP Nitrogen blade servers equipped with Emulex HBAs. The error is seen when Flex-FC mode is enabled on the Emulex HBAs.

**Resolution:** Fixed

## QCCR1D 103913

**Description:** OS Provisioning should support Broadcom NetXtreme IITM 5708 Gigabit Ethernet NICs.

**Platform:** Windows

**Subsystem:** OS Provisioning

**Symptom:** WinPE images used for Windows provisioning need the driver for Broadcom NetXtreme IITM 5708 Gigabit Ethernet NICs.

**Resolution:** Fixed

## QCCR1D 104679

**Description:** VMWare ESX 3.5 OS Provisioning fails on certain HP ProLiant servers due to a disk device name change from `cciss/c0d0` to `sda`.

**Platform:** VMWare ESX 3.5

**Subsystem:** OS Provisioning Backend

**Symptom:** VMWare ESX 3.5 OS Provisioning fails on certain HP ProLiant servers due to a disk device name change from `cciss/c0d0` to `sda`.

**Resolution:** Fixed

## QCCR1D 104764

**Description:** Windows Server 2008 R1 provisioning should support the Abstract PRO/1000 MT Single Port Adapter.

**Platform:** Windows Server 2008 R1

**Subsystem:** OS Provisioning Backend

**Symptom:** Provisioning a Windows Server 2008 R1 fails due to no driver for the Abstract PRO/1000 MT Single Port Adapter.

**Resolution:** Fixed

## Patch Management - Solaris

### QCCR1D 102345

**Description:** During import of Solaris patches, `create_db` fails with the error `UnboundLocalError: local variable 'metaDataFound' referenced before assignment`.

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

**Symptom:** During Solaris patch import, the error `UnboundLocalError: local variable 'metaDataFound' referenced before assignment` occurs and import aborts.

**Resolution:** Fixed

### QCCR1D 103604

**Description:** During Solaris patch import, `show` action returns a traceback error `AttributeError: 'SolPatchBundle' object has no attribute platforms`.

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

**Symptom:** During Solaris patch import, `show` action returns a traceback error `AttributeError: 'SolPatchBundle' object has no attribute 'platforms'`.

**Resolution:** Fixed

## Patch Management - SUSE Linux

### QCCR1D 102109

**Description:** Remediation of Software Policies and Patch Policies fails on SUSE 11x86\_64 platforms.

**Platform:** Independent

**Subsystem:** Patch Management - Suse Linux

**Symptom:** If a managed server is not configured to use a gateway, then hostnames such as "theword" do not resolve correctly.

**Resolution:** Fixed

## Patch Management - Unix

### QCCR1D 83879

**Description:** During AIX Patching, transfer of a large amount of APAR related data degrades core performance.

**Platform:** AIX

**Subsystem:** Patch Management - Unix - Backend

**Symptom:** This issue occurs during the first registration of AIX machines and when applying a substantial patch to a server that is already managed by SA. SA recognizes only individual APARs rather than bundles, products, and MLs. Since bundles, products, and especially MLs can consist of hundred or thousands of APARs, it is quite common for each AIX machine to have thousands or even tens of thousands of APARs associated with it. Each APAR registered represents a database insert and a variety of other actions on the SA core. Each insert must be sent across any mesh and each core in the mesh will also have to perform an insert. Thus, performance is degraded.

**Resolution:** Fixed

### QCCR1D 93840

**Description:** APARFilesetUnit can become incorrectly associated with both BaseFilesetUnit and UpdateFilesetUnit and cause remediation to fail.

**Platform:** AIX

**Subsystem:** Patch Management - Unix - Backend

**Symptom:** Remediation failures occur when trying to install certain APARs.

**Resolution:** Fixed

## Patch Management - Windows

### QCCR1D 102628

**Description:** The server browser does not show any patches for the server and returns an error if the count of all patches in all attached Windows patch policies is 1000 or more.

**Platform:** Independent

**Subsystem:** Patch Management - Windows - Backend

**Symptom:** The server browser does not show any patches for the server and returns the error:  
WindowsPatchService.getDevicePatches returns an ORA-01795 error.

**Resolution:** Fixed

## QCCR1D 105637

**Description:** Windows Server 2008 R2 patching support in SA 7.5.05 and 7.82.

**Platform:** Windows Server 2008

**Subsystem:** Patch Management - Windows - Backend

**Symptom:** SA does not extract Windows Server 2008 patches in SA 7.50.05 and 7.82.

**Resolution:** Fixed

## Red Hat Network Import

### QCCR1D 105106

**Description:** Changes to the Red Hat Network caused `rhn_import` to fail while attempting to download packages.

**Platform:** Solaris, Linux

**Subsystem:** Red Hat Network Import

**Symptom:** User runs `rhn_import` and sees the following error although the RHN credentials are valid:  
RHNetworkAuthError: RHN Error: Login failed - error.invalid\_login.

**Resolution:** Fixed

### QCCR1D 106016

**Description:** Red Hat Network Import fails with an Unexpected error: AttributeError: 'int' object has no attribute 'strip'.

**Platform:** Red Hat Enterprise Linux

**Subsystem:** RHN Import

**Symptom:** Red Hat Network Import fails with the error:

Unexpected error: AttributeError: 'int' object has no attribute 'strip'

**Resolution:** Fixed

## Server Module

### QCCR1D 105360

**Description:** Server Module packages and patches are not working on AIX6.1.

**Platform:** AIX 6.1

**Subsystem:** Server Module - Packages and Patches

**Symptom:** Selecting Registered Software should trigger installation of the Server Module packages and patches via:

- audit
- snapshot
- server browser (inventory)

and return all registered packages and patches on the target server but does not.

**Resolution:** Fixed

## Software Management

### QCCR1D 93946

**Description:** Software policy compliance shows an incorrect number of items when there is a Solaris patch cluster and Cluster children in the policy.

**Platform:** Solaris

**Subsystem:** Software Management - API - Compliance

**Symptom:** Policy compliance shows an incorrect number of items when there are both Solaris patch cluster and Cluster children in the policy.

**Resolution:** Fixed

### QCCR1D 94106

**Description:** During a remediation that includes a software policy created by importing AIX packages, if you select preview then start the job, the job appears to succeed but does not.

**Platform:** AIX

**Subsystem:** Software Management - Backend - Remediate (Other)

**Symptom:** Remediation fails when a software policy created by importing AIX packages is used and preview is selected before starting the job.

**Resolution:** Fixed

### QCCR1D 100046

**Description:** When OPSWpackage\_paths is set, the agent does not attempt to download packages that are missing from the stage directory.

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)

**Symptom:** When OPSWpackage\_paths is set, the agent does not attempt to download packages that are missing from the stage directory.

**Resolution:** Fixed

## QCCR1D 101517

**Description:** Software compliance shown as non-compliant for some remediate jobs.

**Platform:** Independent

**Subsystem:** Software Management - API - Compliance

**Symptom:** Software compliance show as non-compliant for remediate jobs.

**Resolution:** Fixed

## QCCR1D 101673

**Description:** RPM remediation can fail if a newer version is available in the Software Repository.

**Platform:** Linux

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

**Symptom:** Remediation failure with dependency resolution error.

**Resolution:** Fixed

## QCCR1D 102650

**Description:** Remediation of more than 99 servers at the same time throws an immediate error.

**Platform:** Independent

**Subsystem:** Software Management - API - Software Policy

**Symptom:** Remediation of more than 99 servers at the same time throws an immediate error.

**Resolution:** Fixed

## QCCR1D 106460/101961

**Description:** Detaching a Software policy removes the policy but does not remove the software from a server if the Remediate Now option is not selected.

**Platform:** Independent

**Subsystem:** Software Management - API - Software Policy

**Symptom:** When you detach a Software Policy from a server but do not specify Remediate Now, the policy is removed but the software remains on the server.

**Resolution:** Fixed

## QCCR1D 106463/99524

**Description:** Mismatched packages in Install/Uninstall Sequence cause remediation failure.

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)



**Symptom:** If the packages specified in a Software Policy with a split 'Install Sequence'/'Uninstall Sequence' are not an exact match (at least that all of the packages in the install sequence are also in the uninstall sequence), a detach and remediate of the software policy will initially appear to succeed, but the software policy will remain in the view with a red x. Subsequent attempts to remediate the detached policy will fail with a `Will not remove` error, stating that the package was not installed by SA and has never been adopted.

**Resolution:** Fixed

## Virtualization

### QCCR1D 103752

**Description:** When a virtual machine is created on a VMWare ESX 3.5 server using the SA Client, with guest OS "Microsoft Windows Server 2008 (32bit)", OS installation is completed but the Agent is not installed to the server because network is not set.

**Platform:** VMWare ESX 3.5 VM with guest OS Microsoft Windows Server 2008 (32bit)

**Subsystem:** Virtualization - Backend (VMWare)

**Symptom:** When a virtual machine is created on a VMWare ESX 3.5 server using the SA Client, with guest OS "Microsoft Windows Server 2008 (32bit)", OS installation is completed but the Agent is not installed to the server because network is not set.

**Resolution:** Fixed

## Web Services Data Access Engine

### QCCR1D 104013

**Description:** SQL queries used for calculating Device Group local membership can take a long time in large scale environments.

**Platform:** Independent

**Subsystem:** Web Services Data Access Engine (Twist)

**Symptom:** SQL queries used for calculating Local membership take long time in large scale environments. Query speed can be improved by adding a cache table.

**Resolution:** Fixed

## Fixed in SA 7.81

### Agents

#### QCCR1D 82756

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

**Platform:** Solaris

**Subsystem:** Agent Deployment/Upgrade Backends

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

**Resolution:** Fixed

## QCCR1D 92264

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

**Platform:** Virtuozzo

**Subsystem:** Agent Deployment/Upgrade Backends

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

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

**Resolution:** Fixed

## QCCR1D 93169

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

**Platform:** Solaris 10

**Subsystem:** Agent

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

**Resolution:** Fixed

## QCCR1D 93940

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

**Platform:** Windows

**Subsystem:** Agent

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

**Resolution:** Fixed

## QCCR1D 98995

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

**Platform:** Solaris 8 & Solaris 9

**Subsystem:** Agent

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

**Resolution:** Fixed

## QCCR1D 100053

**Description:** Solaris agent does not report MAC address.

**Platform:** Solaris

**Subsystem:** Agent

**Symptom:** Solaris agent does not report MAC address.

**Resolution:** Fixed

## Application Automation Extensions (APXs)

### QCCR1D 93600

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

**Platform:** VMWare ESX/Linux/Solaris

**Subsystem:** MBC/DHCPD

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

**Resolution:** Fixed

### QCCR1D 99364

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

**Platform:** Independent

**Subsystem:** APX - WebApp

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

**Resolution:** Fixed

## Application Configuration

### QCCR1D 93633

**Description:** Snapshots size is too large.

**Platform:** Independent

**Subsystem:** Application Configuration Backend

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

**Resolution:** Fixed

## Audit and Compliance

### QCCR1D 73612

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

**Platform:** Independent

**Subsystem:** Audit and Compliance - Backend

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

**Resolution:** Fixed

### QCCR1D 97634

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

**Platform:** Independent

**Subsystem:** Application Configuration Backend

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

**Resolution:** Fixed

### QCCR1D 90961

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

**Platform:** Independent

**Subsystem:** Audit & Compliance UI

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

**Resolution:** Fixed

### QCCR1D 94467

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

**Platform:** Independent

**Subsystem:** Audit & Compliance Backend

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

**Resolution:** Fixed

### QCCR1D 98718

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

**Platform:** Windows

**Subsystem:** Audit and Compliance

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

**Resolution:** Fixed

## QCCR1D 99537

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

**Platform:** Independent

**Subsystem:** Audit & Compliance Backend

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

**Resolution:** Fixed

## Command Engine (OCC)

### QCCR1D 83027

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

**Platform:** Independent

**Subsystem:** Command Engine - OCC Client Framework

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

**Resolution:** Fixed

### QCCR1D 100078

**Description:** ZIP installation paths - allow special characters in environment variables for Windows x86-64 versions.

**Platform:** Windows x86-64

**Subsystem:** OCC Client Framework

**Symptom:** The Windows x86-64 versions have environment variables for the program file directories which include special characters (parentheses). For example, the environment variable `%ProgramFiles(x86)%` represents the directory `C:\Program Files (x86)`.

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

**Resolution:** Fixed

### QCCR1D 84111

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

**Platform:** Independent

**Subsystem:** OCC Client Framework

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

**Resolution:** Fixed

## Custom Extensions

### QCCR1D 92622

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

**Platform:** Independent

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

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

**Resolution:** Fixed

## Data Access Engine

### QCCR1D 95875

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

**Platform:** Independent

**Subsystem:** Data Access Engine (Spin)

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

**Resolution:** Fixed

### QCCR1D 99604

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

**Platform:** Windows Server 2008 R2

**Subsystem:** Data Access Engine (Spin)

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

**Resolution:** Fixed

## Gateways

### QCCR1D 93982

**Description:** The Gateway (opswgw) chroot environment on Linux x86\_64 is missing the /lib64 directory.

**Platform:** Linux

**Subsystem:** Gateway

**Symptom:** When the Gateway (opswgw) is installed on a Linux x86\_64 system, the /lib64 directory is not created in the opswgw chroot environment. This can prevent the gateway from being able to properly egress proxied TCP connections, failing with a name lookup error.

**Resolution:** Fixed

## Global File System

### QCCR1D 100563

**Description:** Multiple vnodes pointing to the same inode.

**Platform:** Independent

**Subsystem:** Global Filesystem/Shell Backend

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

**Resolution:** Fixed

## Model Repository

### QCCR1D 93757

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

**Platform:** Independent

**Subsystem:** Model Repository (Truth)

**Symptom:** ORA-01000: maximum open cursors exceeded - set cursor\_sharing = exact (shell script)

**Resolution:** Fixed

### QCCR1D 110310

**Description:** In SA 9.0 the Waypurge Garbage Collection PL/SQL code was modified to fix a bug that did not delete all the child records from the session\_service\_instances table.

The CORD bug backports the changes made in SA 9.0 into SA 7.80.03.

**Platform:** Independent

**Subsystem:** Model Repository (Truth)

**Symptom:** Data in the SESSION\_SERVICE\_INSTANCES table is poor because Garbage Collection is not working properly, so the number of records increases over time.

**Resolution:** Fixed

## Networking

### QCCR1D 92622

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

**Platform:** Solaris

**Subsystem:** CX - Single user mode helper

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

**Resolution:** Fixed

## OS Provisioning

### QCCR1D 89237

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

**Platform:** Windows Server 2008/VMWare ESX

**Subsystem:** OS Provisioning - OCC - client

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

**Resolution:** Fixed

### QCCR1D 90094

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

**Platform:** Windows Server 2003

**Subsystem:** OS Provisioning - Backend

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

**Resolution:** Fixed

### QCCR1D 93128

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

**Platform:** Independent

**Subsystem:** OS Provisioning - OCC - Client

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

**Resolution:** Fixed



## QCCR1D 93847

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

**Platform:** Windows Server 2008

**Subsystem:** OS Provisioning Backend

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

**Resolution:** Fixed

## QCCR1D 95918

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

**Platform:** Independent

**Subsystem:** OS Provisioning Backend

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

**Resolution:** Fixed

## QCCR1D 99603

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

**Platform:** Windows Server 2008 SP2

**Subsystem:** OS Provisioning Backend

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

**Resolution:** Fixed

## Patch Management - Solaris

### QCCR1D 90961

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

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

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

**Resolution:** Fixed

## QCCR1D 91806

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

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

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

**Resolution:** Fixed

## QCCR1D 92173

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

**Platform:** Independent

**Subsystem:** Patch Management - Solaris

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

**Resolution:** Fixed

## QCCR1D 92426

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

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

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

**Resolution:** Fixed

## QCCR1D 93225

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

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

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

**Resolution:** Fixed

## Patch Management - Windows

### QCCR1D 79697

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows

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

**Resolution:** Fixed

### QCCR1D 83968

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows - Backend

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

**Resolution:** Fixed

### QCCR1D 90509

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows - UI

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

**Resolution:** Fixed

### QCCR1D 92308

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows

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

**Resolution:** Fixed

## QCCR1D 93393

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows - Backend

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

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

**Resolution:** Fixed

## QCCR1D 93496

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows - Backend

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

**Resolution:** Fixed

## QCCR1D 94132

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

**Platform:** Windows

**Subsystem:** Patch Management - Windows - UI

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

**Resolution:** Fixed

## QCCR1D 97792

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

**Platform:** Independent

**Subsystem:** Patch Management - Windows - Backend

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

**Resolution:** Fixed

## Powershell

### QCCR1D 90201

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

**Platform:** Windows 2003

**Subsystem:** Web Services

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

**Resolution:** Fixed

## SA Client

### QCCR1D 92982

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

**Platform:** Independent

**Subsystem:** Search

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

**Resolution:** Fixed

### QCCR1D 93159

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

**Platform:** Independent

**Subsystem:** Search

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

**Resolution:** Fixed

### QCCR1D 94277

**Description:** URL for the deployed web services is invalid.

**Platform:** Independent

**Subsystem:** Web Services

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

**Resolution:** Fixed

## SAS Web Client

### QCCR1D 70583 (159229)

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

**Platform:** Independent

**Subsystem:** SAS Web Client

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

**Resolution:** Fixed

## Scripts

### QCCR1D 82714

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

**Platform:** Independent

**Subsystem:** DSE (UI)

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

**Resolution:** Fixed

## Server Module

### QCCR1D 83143

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

**Platform:** Independent

**Subsystem:** Server Module - Discovery Modules

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

**Resolution:** Fixed

### QCCR1D 92829

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

**Platform:** Independent

**Subsystem:** Server Module - Backend

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

```
OpwareError: serverCompliance.FailedToCreateSnapshot [module:
com.opware.compliance.server.rmi, method: createSnapshot, line: 219
[...]
```

**Resolution:** Fixed

## QCCR1D 93173

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

**Platform:** Red Hat Enterprise Linux

**Subsystem:** Server Module - Packages and Patches

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

**Resolution:** Fixed

## QCCR1D 94119

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

**Platform:** ESX

**Subsystem:** Server Module - Discovery Modules

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

**Resolution:** Fixed

## QCCR1D 95403

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

**Platform:** Independent

**Subsystem:** Server Module - Backend

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

**Resolution:** Fixed

## QCCR1D 99173

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

**Platform:** Independent

**Subsystem:** Server Module - Backend

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

**Resolution:** Fixed

## Software Management

### QCCR1D 72251

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

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)

**Symptom:** Remediate job completes with the message:

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

**Resolution:** Fixed

### QCCR1D 76594

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

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)

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

**Resolution:** Fixed

### QCCR1D 88615

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

**Platform:** Linux

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

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

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

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

**Resolution:** Fixed

### QCCR1D 90586

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

**Platform:** Independent

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



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

**Resolution:** Fixed

## QCCR1D 93309

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

**Platform:** Solaris

**Subsystem:** Software Management - Backend - Remediate (Other)

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

**Resolution:** Fixed

## QCCR1D 94127

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

**Platform:** Solaris

**Subsystem:** Software Management - Backend - Remediate (Other)

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

**Resolution:** Fixed

## QCCR1D 94379

**Description:** Application Configuration provisioning hangs.

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)

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

**Resolution:** Fixed

## QCCR1D 96839

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

**Platform:** Independent

**Subsystem:** Software Management - API - Compliance

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

**Resolution:** Fixed

## QCCR1D 97790

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

**Platform:** Independent

**Subsystem:** Software Management - API - Software Policy

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

**Resolution:** Fixed

## QCCR1D 100395

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

**Platform:** Linux

**Subsystem:** Software Management - API - Compliance

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

**Resolution:** Fixed

## QCCR1D 100396

**Description:** Software Compliance does not work correctly on x86\_64 platforms.

**Platform:** x86\_64 platforms

**Subsystem:** Software Management - API - Compliance

**Symptom:** Software Compliance does not work correctly on x86\_64 platforms

**Resolution:** Fixed

## QCCR1D 100417

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

**Platform:** Independent

**Subsystem:** Software Management - API - Compliance

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

**Resolution:** Fixed

## QCCR1D 100854

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

**Platform:** Independent

**Subsystem:** Software Management - Backend - Remediate (Other)

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

**Resolution:** Fixed

## Virtualization

### QCCR1D 83067

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

**Platform:** VMware

**Subsystem:** Virtualization - Backend (VMWare)

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

**Resolution:** Fixed

### QCCR1D 89739

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

**Platform:** VMWare

**Subsystem:** Virtualization - Backend (VMWare)

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

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

**Resolution:** Fixed

### QCCR1D 93055

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

**Platform:** Microsoft Hyper-V

**Subsystem:** Virtualization - Microsoft Hyper-V

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

**Resolution:** Fixed

### QCCR1D 93123

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

**Platform:** VMWare

**Subsystem:** Virtualization - UI

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

**Resolution:** Fixed

## QCCR1D 93220

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

**Platform:** ESX

**Subsystem:** Virtualization - UI

**Resolution:** Fixed

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

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

**Resolution:** Fixed

## QCCR1D 93703

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

**Platform:** Independent

**Subsystem:** Virtualization - Backend (VMWare)

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

**Resolution:** Fixed

## QCCR1D 93756

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

**Platform:** Solaris

**Subsystem:** Virtualization - Backend (Zones)

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

**Resolution:** Fixed

## QCCR1D 94076

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

**Platform:** ESX & ESXi

**Subsystem:** Virtualization - Backend (VMWare)

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

**Resolution:** Fixed

## QCCR1D 94207

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

**Platform:** VMWare ESX 3.5

**Subsystem:** Virtualization - Backend (VMWare)

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

**Resolution:** Fixed

## QCCR1D 110493

**Description:** In the SA Client, if you choose **Servers** ► **Virtual Server** panel, Solaris10 x86-64bit VMs are not listed in the Managed Server panel under their ESX servers, even if you perform a VMware VM refresh.

**Platform:** Solaris 10 x86-64bit VMs

**Subsystem:** Storage Host Agent Extension

**Symptom:** Solaris VMs are not displayed under the Managed Server panel.

**Resolution:** Fixed

## Visual Analyzer

### QCCR1D 84313

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

**Platform:** Windows 2008

**Subsystem:** Visual Analyzer - UI

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

**Resolution:** Fixed

## Web Services Data Access Engine

### QCCR1D 83222

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

**Platform:** Independent

**Subsystem:** Web Services Data Access Engine (Spin)

**Symptom:** Internal changes to improve performance required.

**Resolution:** Fixed

## QCCR1D 92819

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

**Platform:** Independent

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

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

**Resolution:** Fixed

## 4 Known Problems, Restrictions, and Workarounds in SA 7.83

The issues in this section are identified by 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.

### Agents

#### QCCR1D 100660

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

**Platform:** Windows Server 2008 using UAC

**Subsystem:** Windows Agent Deployment

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

**Workaround:** Turn off UAC:

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

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

#### QCCR1D 102401

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

**Platform:** All

**Subsystem:** Agent Deployment or Hardware Registration

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

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

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

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

For example, if you received the following error:

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

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

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

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

## Audit and Compliance

### QCCR1D 102706

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

**Platform:** Independent

**Subsystem:** Audit and Compliance

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

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

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

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



# Extensible Discovery APX

## QCCR1D 106467

**Description:** SA Extensible Discovery script `get_firmware_version.sh` requires `dmidecode` and/or `lsmcode` utility to run successfully on Linux.

**Platform:** Linux

**Subsystem:** Content/Extensible Discovery APX

**Symptom:** Without the `dmidecode` or `lsmcode` utilities installed on the managed server, the SA Extensible Discovery extension script `get_firmware_version.sh` will fail to run and present the following error (from QCCR1D 106432):

```
"Error encountered for one or more collection items: Script /var/opt/opsware/
extensible_discovery/scripts/get_firmware_version.sh returned non zero (1).
Here is its output:
Can't find dmidecode and/or lsmcode. Please install this binary on the managed
host. Exiting.
The following server(s) had errors: example.server.hp.com"
```

**Workaround:** Ensure that the `dmidecode` (x86) and/or `lsmcode` (PPC) utilities are installed on the managed host to dump BIOS/firmware information on Linux. On Red Hat Linux, this utility is provided as part of the `kernel-utils` (x86) or `ppc64-utils` (PPC) RPMs. On SuSE Linux, this is provided in the `pmtools` (x86) or `lsvpd` (PPC) RPMs.

# Global File System

## QCCR1D 93497

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

**Platform:** Solaris

**Subsystem:** Global File System/Shell Backend

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

**Workarounds:**

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

# Hyper-V

## QCCR1D 97630

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

**Platform:** Windows

**Subsystem:** Hyper-V

**Symptom:** Multi-master conflicts occur.

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

## QCCR1D 98310

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

**Platform:** Windows

**Subsystem:** Hyper-V

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

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

```
<IP-address> <FQDN>
```

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

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

## QCCR1D 101449

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

**Platform:** Windows

**Subsystem:** Hyper-V

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

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

## QCCR1D 102344

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

**Platform:** Windows

**Subsystem:** Hyper-V

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

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

## Model Repository

### QCCR1D 93757

**Description:** ORA-01000: maximum open cursors exceeded - set cursor\_sharing = exact (shell script).

**Platform:** Independent

**Subsystem:** Model Repository/Oracle RDBMS 11.1.0.7

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

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

**Workaround:** With SA 7.83, a script is provided that modifies the TRUTH database user's dba\_job that collects the schema statistics. Perform the following tasks to apply this workaround:

#### Copying the Script

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

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

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

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

#### Running the Script

The following is required to run the script:

- You must run the script as root

You will also need the following information:

- ORACLE\_HOME
- ORACLE\_SID
- Password for the schema owner TRUTH

*Script usage*

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

For example:

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

## QCCR1D 96568

**Description:** Cannot duplicate a zip package.

**Platform:** Independent

**Subsystem:** Model Repository - Truth

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

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

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

```
truth_unit_folder_trigs.sh
```

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

- UNIT\_SHADOW\_FLDR\_AS\_RTRG on the UNIT\_RELATIONSHIPS table
- FLD\_UNIT\_SHADOW\_FLD\_UNIT\_RTRG on the FOLDER\_UNIT table

After modifying the triggers, the script processes any unprocessed data in SHADOW\_FOLDER\_UNIT table.

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

- /opsware\_installer/tools/truth\_unit\_folder\_trigs.sh
- /opsware\_installer/tools/truth\_unit\_folder\_trigs.sql

For example:

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

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

- ORACLE\_HOME
- ORACLE\_SID
- The password for schema owner TRUTH

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

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

For example:

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

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

Task completed

### Rollback

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

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

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

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

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

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

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

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

For example:

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

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

Task completed.

## QCCR1D 111642

**Description:** After applying the `truth_create_local_dc_table.sh` script, System Diagnosis displays an error.

**Platform:** Independent

**Subsystem:** Model Repository - Truth

**Symptom:** After running the `truth_create_local_dc_table.sh` script to create the `LOCAL_DC_TABLE`, you may see the following error when running the System Diagnostic test on your core:

```
Test Name: Model Repository Schema  
Description: Verifies that the Data Access Engine's version of the schema  
matches the Model Repository's version.  
Component device: Data Access Engine (spin)  
Test Results: The following tables differ between the Data Access Engine and  
the Model Repository: local_data_centers.
```

**Workaround:** This error is incorrect and you can disregard it.

# OS Provisioning

## QCCR1D 93849

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

**Platform:** Linux

**Subsystem:** OS Provisioning - Reprovisioning

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



---

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

---

**Workaround:** Ensure that:

- 1 `truth.dcDispNm` and `truth.dcNm` are same string.
- 2 `truth.dcDispNm` is specified as all caps (for example, `SILICA`, not `silica`).

## QCCR1D 101920

**Description:** Solaris 10 packages are only partially installed.

**Platform:** Solaris

**Subsystem:** OS Provisioning Backend

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

**Workaround:** Copy the file:

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

from your Solaris 10 boot media, into the directory:

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

## QCCR1D 102449

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

**Platform:** Windows Server 2008 R2

**Subsystem:** OS Provisioning Backend

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

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

**Workaround:**

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

## QCCR1D 111445

**Description:** Run OS Sequence does not escalate device group permission.

**Platform:** Independent

**Subsystem:** OS Provisioning

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

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

## Patch Management: Solaris

### QCCR1D 95745

**Description:** When resolving the dependencies for a set of Solaris patches in a patch policy, the incompatible patches dialog may repeatedly be displayed. This can occur when an incompatible patch is required by another patch in the patch policy or when an incompatible patch obsoletes another patch in the patch policy. After you specify an incompatible patch to be removed from the policy, it may get added back because it is required by some other patch in the policy, resulting in the incompatible patches dialog being redisplayed.

**Platform:** Solaris

**Subsystem:** Solaris Patching

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

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

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

### QCCR1D 98409

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

**Platform:** Solaris

**Subsystem:** Solaris Patching

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

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

## QCCR1D 100566

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

**Platform:** Solaris

**Subsystem:** Solaris Patching

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

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

## QCCR1D 101449

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

**Platform:** Solaris

**Subsystem:** Solaris Patching

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

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

## QCCR1D 104468

**Description:** When the “Manage Packages” permission is set to “Read”, the `solpatch_import` command incorrectly allows you to modify the Solaris patch database.

**Platform:** Solaris

**Subsystem:** Solaris Patching

**Symptom:** When the “Manage Packages” permission is set to “Read”, the `solpatch_import` command incorrectly allows you to modify the Solaris patch database, for example by importing Solaris patches into the Solaris patch database. These operations should only be allowed when the “Manage Packages” permission is set to “Read and Write”.

For more information on permissions, see “Patch Management for Solaris” in the *SA User Guide: Application Automation* and the *SA Administration Guide*.

**Workaround:** None



## QCCR1D 106844

**Description:** solpatch\_import only supports the importing of complete bundles (that is, not individual parts or bundles with missing parts).

**Platform:** Solaris

**Subsystem:** Patch Management - Solaris

**Symptom:** When using solpatch\_import to import a bundle with missing parts, the following error can occur:

```
Unexpected error: Traceback (most recent call last):
File "./bin/solpatch_import_versioned.py", line 3567, in main
File "./bin/solpatch_import_versioned.py", line 2689, in doImport
File "./bin/solpatch_import_versioned.py", line 1920, in _importBundle
File "./libsolpatch.py", line 2108, in loadBundleMetadata
File "./libsolpatch.py", line 1959, in _readBundleRawMetaFiles AssertionError
```

**Workaround:** Try the import again and ensure that all parts of the bundle are downloaded at the beginning of the import. If any of the parts are not downloaded, the import will fail with the above error.

## QCCR1D 111601

**Description:** All bundles with new names show Will Not Install with reason not applicable to server.

**Platform:** Solaris

**Subsystem:** Solaris Patching

**Symptom:** Cannot install Solaris clusters/bundles after upgrade to SA 7.83.

**Workaround:** Sun recently changed the naming conventions it uses for clusters/bundles provided on the SunSolve website (<http://sunsolve.sun.com>). Therefore, SA 7.83 provides a new collection file (also available through HP Live Network (HPLN)). After the new collection file is installed, it triggers an update to the current Solaris cluster/bundle names displayed in the SA Client and modifies the solpatch\_import script to use the new cluster/bundle names when downloading from SunSolve. To be sure all clusters/bundles information is properly updated in the database, before attempting to use solpatch\_import to create policies and/or import clusters or bundles, run:

```
./solpatch_import -a update_supplements
```

## QCCR1D 111692

**Description:** You cannot import a new version of a Solaris patch bundle into the SA Library if the old version is in the SA Library.

**Platform:** Solaris

**Subsystem:** Solaris Patching

**Symptom:** If you attempt to import a new version of a Solaris patch bundle into the SA Library when the old version is in the SA Library, the import will skip the bundle and report that it already exists in the SA Library.

**Workaround:** Delete the old version of the Solaris patch bundle, then import the new version. For more information, see “Patch Management for Solaris” in the *SA User Guide: Application Automation*.

## Patch Management: Unix

### QCCR1D 106847

**Description:** When using the `import_aix_packages` script, you see an error similar to the following recurring frequently:

```
Feb 13 01:44:06 INFO [8864]: [680/680] Importing U831579.bff
Feb 13 01:44:06 ERROR [8864]: Opsware error (cogbot.packageFormatError):
Invalid LPP file
Feb 13 01:44:06 ERROR [8864]: Opsware error (cogbot.packageFormatError):
Invalid LPP file
Feb 13 01:44:06 ERROR [8864]: Opsware error (cogbot.packageFormatError):
Invalid LPP file
```

**Platform:** AIX

**Subsystem:** Patch Management - Unix

**Symptom:** An invalid LPP file causes an import error.

**Workaround:** Delete the invalid LPP file that causes the error and try the import again.

## Permissions

### QCCR1D 101710

**Description:** Clone Server Permission is obsolete.

**Platform:** Independent

**Subsystem:** Permissions, Server Management

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

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

## SA Client

### QCCR1D 105630

**Description:** Requirement to install newer version of the SA Client Launcher for SA 7.82

**Platform:** Windows

**Subsystem:** SA Client — Launcher

**Symptom:** If you install the SA 7.82 patch and are using a pre-1.3.8 version of the SA Client Launcher to connect to a 7.82 core, you will get a message stating that you must download and install version 1.3.8 of the launcher. The 1.3.8 launcher is also required for support of Windows 7.

**Workaround:** Before using the SA Client Launcher to connect to a 7.82, uninstall the older version of the launcher, visit the Login page of the SAS Web Client, and then download and install version 1.3.8 of the launcher.

## Satellites

### QCCR1D 97659

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

**Platform:** Windows

**Subsystem:** Satellites

**Symptom:** Network scans fail with an error.

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

## Software Management

### QCCR1D 100754

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

**Platform:** All

**Subsystem:** Software Management

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

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

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

**Workaround:** None

# Software Repository

## QCCR1D 99828

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

**Platform:** Independent

**Subsystem:** Software Repository

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

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

# Virtualization

## QCCR1D 93492

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

**Platform:** VMware

**Subsystem:** VMware Console

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

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

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

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

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

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

## 5 Documentation Errata

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

### SA 7.82 Release Notes

In the Pre-Patch step of the Installation Procedure, the path to the pre-patch script given as:

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

should be

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

and, the path to the rollback script given as:

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

should be:

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

### *SA Planning and Installation Guide*

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

#### Chapter 1: SA Core Component Bundling (page 15)

The sentence in the first paragraph that reads:

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

should read:

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

#### Chapter 2: Pre-Installation Requirements (page 55)

In the section “SUSE Linux Enterprise Server 10 Package Requirements”, add the following:

The following packages *must not* be installed on a SUSE Linux Enterprise Server 10 hosting an SA Core:

- yast2-dhcp-server

- rsync
- samba
- samba-32bit
- yast2-samba-server
- yast2-tftp-server



---

These packages are reinstalled during an operating system upgrade from SP2 to SP3 and therefore must be removed for proper SA Core operation

---

## Chapter 3: Solaris Requirements (page 48)

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

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

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

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

## Chapter 3: SUSE Enterprise Server 10 Requirements

The following are package requirements for SUSE Enterprise Server Linux 10.

### Required SUSE Linux Enterprise Server 10 Packages

For SUSE Linux Enterprise Server 10 64-bit x\_86, an SA Core Server must have the packages listed in [Table 1](#) installed.

**Table 1** SUSE Linux Enterprise Server 10 Required Packages

Required Packages	Architecture
binutils	x86_64
cpp	x86_64
desktop-file-utils	x86_64
expat	x86_64
gcc-c++	x86_64
gcc	x86_64
glibc	x86_64
glibc-32bit	x86_64
glibc-devel	x86_64
glibc-devel-32bit	x86_64
iptables	x86_64
kernel-smp	x86_64
kernel-source	x86_64
libaio	x86_64
libaio-32bit	x86_64
libaio-devel	x86_64
libcap	x86_64
libcap-32bit	x86_64
libelf	x86_64
libgcc	x86_64
libstdc++	x86_64
libstdc++-devel	x86_64
libpng	x86_64
libpng-32bit	x86_64
libxml2	x86_64

**Table 1 SUSE Linux Enterprise Server 10 Required Packages (cont'd)**

<b>Required Packages</b>	<b>Architecture</b>
libxml2-32bit	x86_64
libxml2-python	x86_64
make	x86_64
mDNSResponder-lib	x86_64
mkisofs	x86_64
ncompress	x86_64
nfs-utils	x86_64
patch	x86_64
popt	x86_64
popt-32bit	x86_64
readline	x86_64
readline-32bit	x86_64
rpm	x86_64
sharutils	x86_64
strace	x86_64
sysstat	x86_64
termcap	x86_64
unzip	x86_64
vim	x86_64
xinetd	x86_64
xntp	x86_64
xorg-x11-libs	x86_64
xorg-x11-libs-32bit	x86_64
xorg-x11	x86_64
xterm	x86_64
zip	x86_64
zlib	x86_64
zlib-32bit	x86_64



Table 2 shows packages *must not* be installed on a SUSE Linux Enterprise Server 10 hosting an SA Core:

**Table 2 Packages Not Supported on SUSE Linux Enterprise Server 10 Core Hosts**

Package	Package
rsync	yast2-dhcp-server
samba	yast2-samba-server
samba-32bit	yast2-tftp-server



These packages are reinstalled during an operating system upgrade from SUSE Enterprise Linux SP2 to SP3 and therefore must be removed for proper SA Core operation after upgrade.

## Appendix A: Table 42 (Page 188)

In **Table 42: Supported Operating Systems and Oracle Versions**, the first entry, SunOS 10 x86\_64, should read, SunOS 10 (SPARC)-64 bit.

## Appendix A: Solaris Requirements (page 190)

In the bulleted entry that reads:

- Free /tmp space should be 400MB or more

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

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

the command should read:

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

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

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

### Both Oracle 10g and 11g

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

### Oracle 10g only

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

## Oracle 11g only

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

## Appendix A: Changing Kernel Parameter Values for Linux (page 198)

- 1 Add the following note:



---

For Oracle 11g, the typical number of open file descriptors used under normal usage has increased. For larger systems, HP recommends that you increase the value of `fs.file-max`. The recommended value is `fs.file-max = 681574`

---

- 2 Change the following entry in the Oracle parameter list:

```
fs.file-max=65536  
  
to  
  
fs.file-max = 681574
```

## SA Upgrade Guide

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

The sentence that reads:

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

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

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

This step should read:

Select `Multimaster Opware Core - Subsequent Core`

Chapter 3: Phase 6 (page 50)

A step is missing after Step 3:

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

The existing Step 4 should be renumbered Step 5.

## SA Policy Setter Guide

In the *SA Policy Setter's Guide* "Operating System Provisioning Setup" chapter, the section titled: "Solaris Provisioning from a Boot Server on a Red Hat/SLES 10 Linux Server — Disabling NFS v3 or NFS v4" has incorrect instructions and needs to be changed.

### Incorrect Instructions:

To disable NFS v4 on an SLES 10 Boot Server host:

- 1 On the Boot Server host, create the following file:  
`/etc/sysconfig/nfs`
- 2 In the newly created NFS file, add the following line:  
`NFS4_SUPPORT="no"`
- 3 Restart NFS:  
`/etc/init.d/nfs stop`  
`/etc/init.d/nfs start`

### Correct Instructions:

To disable NFS v4 on an SLES 10 Boot Server host:

- 1 On the Boot Server host, create the following file:  
`/etc/sysconfig/nfs`
- 2 In the newly created NFS file, add the following line:  
`NFS4_SUPPORT="no"`
- 3 Restart NFS:  
`/etc/init.d/nfsserver restart`

## Users Guide: Application Automation, OS Provisioning, Manage Boot Clients (MBC)

Required Permissions: In addition the permissions listed for the Manage Boot Clients (MBC) utility, you also need the following permission: *Read & Write permission to customer Not Assigned.*

## Oracle RAC Support: *Oracle Setup for the Model Repository/ SA Planning and Installation Guide, Appendix A*

The following information is in addition to that found in the *SA Planning and Installation Guide: Appendix A* and the document, *Oracle Setup for the Model Repository.*

Concurrent with the SA 7.82 patch release, SA adds support for Oracle Real Application Clusters (RAC).



---

Oracle RAC support requires a new installation of both Oracle and SA. Therefore, in order to enable Oracle RAC support in SA, you must first install SA 7.80 and Oracle 10.2.0.4 or 11.1.0.7 configured as described in the following sections.

---

## Supported Oracle Versions Matrix

### Supported Oracle Versions:

SA support for Oracle RAC includes these Oracle Enterprise Edition versions:

- 10.2.0.4
- 11.1.0.7

### Supported Operating Systems

- Red Hat Enterprise Linux AS 4 x86\_64
- Red Hat Enterprise Linux AS 5 x86\_64

## Set up the Oracle RAC database/instances

SA supports any valid Oracle RAC configuration, such as any number of nodes, ASM or regular disks, and so on.

However, SA requires that the Oracle database be configured for use with SA. You will require your Oracle DBA's help to configure the Oracle RAC/instances, the required initialization parameters, the required tablespaces, the `opsware_admin` database user, and the `listener.ora` and `tnsnames.ora` files.

You can also run the `truth_oracle_state_checker` script to check if the initialization parameters are set correctly. The `truth_oracle_state_checker` file is located in the distribution `/tools` directory.

### Create the Database with the Required Initialization Parameters

Before installing Oracle, the following scripts must be run and `init.ora` must have certain parameter values edited or added as shown in [Required and Suggested Parameters for init.ora](#) on page 125.

- 1 Create a database with the UTF8 character set (as required by SA), the data and index files, the default temporary tablespace, the undo tablespace, and the log files.

### Create the required table spaces

- 2 Create the following tablespaces that are required by SA:

```
LCREP_DATA
LCREP_INDX
TRUTH_DATA
TRUTH_INDX
AAA_DATA
AAA_INDX
AUDIT_DATA
AUDIT_INDX
STRG_DATA
STRG_INDX
```

See “Tablespace Sizes” in the *SA Planning and Installation Guide* for additional tablespace sizing information.

## Required and Suggested Parameters for init.ora

3 The file `init.ora` must be edited as follows:

(Both Oracle 10g and 11g) For SA, the following `init.ora` entries are either suggested or required:

```
log_buffer>=1048576
db_block_size>=8192
session_cached_cursors=>50
nls_length_semantics=CHAR
nls_sort=GENERIC_M
processes >=1024
undo_management=AUTO (Suggested)
undo_tablespace=UNDO (Suggested)
query_rewrite_integrity=TRUSTED
query_rewrite_enabled=true
optimizer_mode=all_rows
optimizer_index_cost_adj=20
optimizer_index_caching=80
cursor_sharing=SIMILAR (value can be set to SIMILAR(preferred) or EXACT,
recommended only if you encounter an Oracle error)
recyclebin=OFF
event="12099 trace name context forever, level 1"
_complex_view_merging=false
```

(Oracle 10g only) For SA, the following `init.ora` entries are either suggested or required:

```
open_cursors >=300
sga_max_size >=1GB
db_cache_size>=629145600
shared_pool_size>=262144000
java_pool_size>=52428800
large_pool_size>=52428800
job_queue_processes>=10
sessions >=1152
pga_aggregate_target >=104857600
workarea_size_policy=auto
remote_login_passwordfile=EXCLUSIVE
```

(Oracle 11g only) For SA, the following `init.ora` entries are either suggested or required:

```
memory_target=1616M
job_queue_processes>=1000 (default)
remote_login_passwordfile=EXCLUSIVE
```

## Create the User `opsware_admin`

4 You can use the script, `CreateUserOpsware_Admin.sql`, to create the `opsware_admin` database user and grant permissions (privileges) to the user (required by SA) or create the user manually.

If you plan to create the `opsware_admin` user manually, follow the procedure below:

### Manual Creation of the User `Opsware_Admin`

To create the `opsware_admin` user after a manual Oracle installation, log in to SQL\*Plus and enter the following:

```

# Su - oracle
# Sqlplus "/" as sysdba"

SQL> create user opsware_admin identified by opsware_admin
      default tablespace truth_data
      temporary tablespace temp
      quota unlimited on truth_data;

SQL> grant alter session to opsware_admin with admin option;
grant create procedure to opsware_admin with admin option;
grant create public synonym to opsware_admin with admin option;
grant create sequence to opsware_admin with admin option;
grant create session to opsware_admin with admin option;
grant create table to opsware_admin with admin option;
grant create trigger to opsware_admin with admin option;
grant create type to opsware_admin with admin option;
grant create view to opsware_admin with admin option;
grant delete any table to opsware_admin with admin option;

grant drop public synonym to opsware_admin with admin option;
grant select any table to opsware_admin with admin option;
grant select_catalog_role to opsware_admin with admin option;
grant query rewrite to opsware_admin with admin option;
grant restricted session to opsware_admin with admin option;

grant execute on dbms_utility to opsware_admin with grant option;
grant analyze any to opsware_admin;
grant insert, update, delete, select on sys.aux_stats$ to opsware_admin;
grant gather_system_statistics to opsware_admin;
grant create job to opsware_admin;

grant alter system to opsware_admin;
grant create role to opsware_admin;
grant create user to opsware_admin;
grant alter user to opsware_admin;
grant drop user to opsware_admin;
grant create profile to opsware_admin;
grant alter profile to opsware_admin;

grant drop profile to opsware_admin;

```

## Installing the Model Repository

In most production environments with Oracle RAC, the Model Repository installation can be done from any SA server. The database server or RAC nodes in this case are considered to be remote.

The examples used in the following sections assume this configuration:

Two (active-active) Node RAC environment:

```

# Public Network
192.168.173.210 rac1pub rac1pub.dev.opsware.com (instance_name=truth1,
db name=truth)
192.168.173.211 rac2pub rac2pub.dev.opsware.com (instance_name=truth2,
db name=truth)

```

```

# Private network
172.16.1.100 rac1prv rac1prv.dev.opsware.com
172.16.1.101 rac2prv rac2prv.dev.opsware.com

# Public Virtual IP (VIP)
192.168.173.212 rac1-vip rac1-vip.dev.opsware.com
192.168.173.213 rac2-vip rac2-vip.dev.opsware.com

SA server:
192.168.173.214 rac1sa.dev.opsware.com

```

## Model Repository Installation on a Remote Database (truth) RAC Server

In an Oracle RAC environment, only one of the RAC nodes is used during the SA installation/upgrade process. The SA Installer connects to only one Oracle RAC instance to install/modify the Model Repository. During the regular SA operations, all RAC nodes are used.

Perform the following tasks on the SA server on which you will run the SA Installer, for example rac1sa.dev.opsware.com.

### Model Repository Hostname Resolution

- 1 On the server where you will run the SA Installer, ensure that the Model Repository hostname truth resolves to the remote database server, not to the server on which you will be running the SA Installer:

In /etc/hosts, enter the public IP address of one of the RAC nodes/instances. For example the /etc/hosts file on rac1sa.dev.opsware.com would have the following entry:

```
192.168.173.210 truth rac1pub rac1pub.dev.opsware.com
```

### Install the Oracle 11g Full Client on the SA server

- 1 The SA Installer will use the Oracle Full Client to connect to the SA server and install the Model Repository. Below are sample commands for installing the Oracle full client.

Create user oracle for the Oracle Full Client installation:

```

root@rac1sa ~]# mkdir -p /u01/app/oracle
root@rac1sa ~]# mkdir -p /u01/app/oraInventory
root@rac1sa ~]# groupadd oinstall
root@rac1sa ~]# groupadd dba
root@rac1sa ~]# useradd -c "Oracle Client software owner" -g oinstall -G
dba -d /u01/app/oracle -s /bin/bash oracle
root@rac1sa ~]# chown -R oracle:oinstall /u01/app
root@rac1sa ~]# chmod -R 775 /u01/app
root@rac1sa ~]# passwd oracle (change oracle user password )

```

- 2 Create the .bash\_profile file.

In /u01/app/oracle create the .bash\_profile file.




---

Temporarily comment out ORACLE\_HOME and ORACLE\_PATH. You will uncomment these entries after the Oracle client installation is complete.

---

Sample .bash\_profile file

```

# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then

```

```

. ~/.bashrc
fi

# User specific environment and startup programs
PATH=$PATH:$HOME/bin
export PATH

#SA-OracleRAC parameters begin
#unset USERNAME
export ORACLE_BASE=/u01/app/oracle
#export ORACLE_HOME=$ORACLE_BASE/product/11.1.0/client_1
#PATH=$ORACLE_HOME/bin:$ORACLE_HOME/OPatch:$PATH
export PATH

if [ -t ]; then
stty intr ^C
fi

umask 022
#SA-OracleRAC parameters end

```

### 3 Install the Oracle Full Client

Install the Oracle Full Client as described in your Oracle documentation. You can create a share to access the Oracle Full Client binaries.

### 4 Set Up Terminals

You will need two X window terminals to install the Oracle Full Client:

Terminal 1: log in as root and enter the commands:

```
Terminal 1> xhost +
```

```
Terminal 2: ssh -X oracle@<new_oracle_full_client_host>
```

### 5 Start Oracle Full Client installation

From Terminal 2 run the Oracle Universal Installer (OUI) installer. The Oracle Full Client is installed in:

```
/u01/app/oracle/product/11.1.0/client_1
```

### 6 Run the Oracle Universal Installer to install Oracle Full Client. The directories in this example assume an Oracle 11g Full Client on Linux.

**a** `cd /location_of_oracle_full_client`

**b** `/runInstaller`

**c** At the **Welcome** Screen, click **Next**.

**d** Specify the Inventory Directory and Credentials (`/u01/app/oraInventory` and `/u01/app/oinstall`)

**e** For **Select Installation Type**, choose Administrator, click **Next**.

**f** For ORACLE\_BASE select: `/u01/app/oracle`, click **Next**.

**g** The Oracle Universal Installer performs some checks. If the checks are not successful, fix the issue and re-run this step. If the checks are successful the click on 'Next'

**h** Oracle OUI will list of products that will be installed. Click on 'Install'

**i** OUI will show the progress bar when installing



- j On the ‘Welcome to Oracle Net Configuration Assistant’ window click on ‘Next’
- k Click on ‘Finish’ once the installation is complete.
- l The following two configuration scripts need to be executed as “root” upon installation being complete:
  - /u01/app/oraInventory/orainstRoot.sh
  - /u01/app/oracle/product/11.1.0/client\_1/root.sh

- 7 Verify that the .bash\_profile file for user oracle is correct.
- 8 Uncomment \$ORACLE\_HOME and \$ORACLE\_PATH.

### Making changes to tnsnames.ora on SA server

By default the tnsnames.ora file is located in /var/opt/oracle.

- 1 Login as root on the SA Server.
- 2 Enter the command:
 

```
mkdir -p /var/opt/oracle
```
- 3 Copy tnsnames.ora from the remote database server to the directory you created above. For the RAC environment, copy it from RAC Node 1 (for example, rac1pub.dev.opsware.com).

The SA Installer puts the database in a restricted mode during the Model Repository installation. The database is removed from the restricted mode after successful installation/upgrade of the Model Repository. When the database is in restricted mode, only certain privileged users are allowed to connect to the database.

To accommodate the remote Model Repository installation process, two sets of tnsnames.ora are required on the SA server.

- tnsnames.ora-install\_upgrade – this copy of tnsnames.ora is used during SA installation/upgrade. The file can be renamed.
- tnsnames.ora-operational – this copy of tnames.ora is used during normal SA operation. The file can be renamed.

You can use softlinks to point tnsnames.ora to either tnsnames.ora-install\_upgrade or tnsnames.ora-operational.

```
ln -s tnsnames.ora-install_upgrade tnsnames.ora
```

### tnsnames.ora-install\_upgrade sample file

Make a note of the text that is in BOLD letters. The tnames.ora file should contain the SID and not the service name. These examples have TRUTH as the truth.servicename. Ensure that the HOST references the same server as the truth entry in /etc/hosts file. truth.servicename is case sensitive.

```
# Generated by Oracle configuration tools.
```

```

TRUTH =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1pub.dev.opsware.com)(PORT = 1521))
    (CONNECT_DATA =
      (SID = truth1)
    )
  )

LISTENER_TRUTH =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1pub.dev.opsware.com)(PORT = 1521))
    (CONNECT_DATA =

```

```

        (SID = truth1)
    )
)

```

Use softlinks to link the file to `tnsnames.ora` file. Do this before you start the SA Model Repository installation or upgrade

```
ln -s tnsnames.ora-install_upgrade tnsnames.ora
```



During installation the SA Installer adds a SA Gateway entry into `tnsnames.ora` (linked to `tnsnames.ora.install-upgrade`) file on the primary SA Core. When installation completes, copy this entry into the `tnsname.ora.operational` file. If this entry is not present in `tnsname.ora.operational`, Multimaster Mesh transactions will not flow. Below is a sample gateway entry from `tnsnames.ora`:

```
Rac2sa_truth=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)(PORT=20002)
(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

### Making changes to listener.ora on one of the RAC node server (instance)

In an Oracle RAC environment, only one of the RAC nodes or instances is used during installation/upgrade process. The SA Installer connects to only one Oracle instance to modify the Model Repository. During the regular SA operations, all the RAC nodes are used.

The SA Installer puts the database in a restricted mode during the Model Repository installation. The database is removed from the restricted mode after successful installation/upgrade of the Model Repository. When the database is in restricted mode, only certain privileged users are allowed to connect. To accommodate the remote truth installation process, two sets of `listener.ora` files are required on the SA server. The files can be given any name. By default the `listener.ora` files are located in `$ORACLE_HOME/network/admin`.

- `listener.ora-install_upgrade` – this copy of `listener.ora` is used during SA install/upgrade
- `listener.ora-operational` – this copy of `listener.ora` is used during normal SA operation.

You can use softlinks to point `listener.ora` to either `listener.ora-install_upgrade` or `listener.ora-operational`:

```
ln -s listener.ora-install_upgrade listener.ora
```

### Sample Listener.ora-install\_upgrade

This file is used during the SA installation/upgrade process. Make a note of the text that is in BOLD letters. The `listener.ora` file should contain the `SID_NAME` and not the service name. The `SID_NAME` is case sensitive. Ensure that the `listener.ora` changes are made on the same server that is referenced in SA servers `/etc/hosts` file.

This example uses `LISTENER_RAC1PUB` as the listener name.

```
# Generated by Oracle configuration tools.
LISTENER_RAC1PUB =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
      (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT =
1521)(IP = FIRST))
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.173.210)(PORT = 1521)(IP =
FIRST))
    )
  )
)
```

```

SID_LIST_LISTENER_RAC1PUB =
  (SID_LIST =
    (SID_DESC=
      (SID_NAME=truth1)
      (ORACLE_HOME=/u01/app/oracle/product/11.1.0/db_2)
    )
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /u01/app/oracle/product/11.1.0/db_2)
      (PROGRAM = extproc)
    )
  )
)

```

You can use softlinks to link the file to `listener.ora`:

```
ln -s listener.ora-install_upgrade listener.ora.ora
```

Ensure that you start the listener as follows:

```
> lsnrctl start LISTENER_RAC1PUB
```

### Testing connection from SA machine to database

Before starting the Model Repository installation/upgrade, you can perform the following tests to verify that your `tnsnames.ora` and `listener.ora` files are configured correctly and if the SA Installer can connect to the database in restricted mode.

- 1 Verify that the SA server's `/var/opt/oracle/tnsnames.ora` file is configured correctly as described in [Making changes to tnsnames.ora on SA server](#) on page 129.
- 2 Verify that the database servers or RAC node's `$ORACLE_HOME/network/admin/listener.ora` file is configured correctly as described in [Making changes to listener.ora on one of the RAC node server \(instance\)](#) on page 130.
- 3 On the SA server:
  - a Login as `oracle` or `root` or `su - twist/spin` – if these users exist
  - b `export ORACLE_HOME=/u01/app/oracle/product/11.1.0/client_1` (or where you installed the Oracle Full Client)
  - c `export LD_LIBRARY_PATH=$ORACLE_HOME/lib`
  - d `export TNS_ADMIN=/var/opt/oracle`
  - e `set $PATH $ORACLE_HOME/bin path`
  - f `sqlplus sys/password@truth as sysdba;`  
where `truth` is the `service_name` or entry from the `tnsnames.ora` file
  - g `select logins from v$instance;`
  - h `alter system enable restricted session;`
  - i `select logins from v$instance;`  
? db should be restricted
  - j `connect opsware_admin/<password>@truth`

If you are able to logon to the database then all files are configured correctly.

- k `sqlplus sys/password@truth as sysdba`
- l `alter system disable restricted session;`

### SA Installer Response File

You can now start the installation of the SA Model Repository. Ensure that you have the correct parameters values for the installation interview or that you have a previous response file.

Verify the paths to the client's `tnsnames.ora` file (`%truth.tnsdir`), oracle client home (`%truth.orahome`), listener port (`%truth.port`), and so on.

- `%truth.tnsdir=/var/opt/oracle`
- `%truth.orahome=/u01/app/oracle/product/11.1.0/client_1`
- `%truth.port=1521`

You can now install the SA Core as described in the *SA Planning and Installation Guide*.

## Post SA installation process

After you install the SA Core, perform the following tasks in order to use all the nodes in the Oracle RAC environment.

### Making changes to `tnsnames.ora` on the SA server

After SA install is complete, the `tnsnames.ora` file should point/link to the `tnsnames.ora-operational` file.

The SA Installer puts the database in a restricted mode during the Model Repository installation. The database is removed from the restricted mode after successful installation/upgrade of the Model Repository. When the database is in restricted mode, only certain privileged users are allowed to connect to the database. To accommodate the remote truth installation process, two sets of `tnsnames.ora` are required on the SA server.

- `tnsnames.ora-install_upgrade` – this copy of `tnsnames.ora` is used during SA installation/upgrade. You can rename the file.
- `tnsnames.ora-operational` – this copy of `tnames.ora` is used during normal SA operation. You can rename the file.

You can use softlinks to point `tnsnames.ora` to either `tnsnames.ora-install_upgrade` or `tnsnames.ora-operational`:

```
ln -s tnsnames.ora-operational tnsnames.ora
```

#### **tnsnames.ora-operational sample file**

Make a note of the text that is in BOLD letters. This `tnsnames.ora` file is used during normal SA operation and contains the RAC parameters.

#This entry is for connecting to RAC virtual machines.

```
TRUTH =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = truth)
      (FAILOVER_MODE =
        (TYPE = SELECT)
        (METHOD = Preconnect)
        (RETRIES = 180)
        (DELAY = 5))
```

```

)
)

LISTENERS_TRUTH =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
  )

#This entry is for connecting to node2 via service_name. This entry is
optional
TRUTH2 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = truth)
      (INSTANCE_NAME = truth2)
    )
  )
)
)
LISTENER_TRUTH2 =
  (ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))

#This entry is for connecting to node1 via service_name. This entry is
optional
TRUTH1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = truth)
      (INSTANCE_NAME = truth1)
    )
  )
)
)
LISTENER_TRUTH1 =
  (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))

```

Use softlinks to link the file to `tnsnames.ora` file after SA installation is complete and you are ready to start SA in operational mode.

```
ln -s tnsnames.ora- operational tnsnames.ora
```



During installation the SA Installer adds an SA Gateway entry into `tnsnames.ora` (linked to `tnsnames.ora.install-upgrade`) file on the primary SA Core. When installation is complete, copy that entry into `tnsname.ora.operational`. If this entry is not present in the `tnsname.ora.operational`, Multimaster Mesh transactions will not flow. The following is a sample gateway entry from `tnsnames.ora`:

```
Rac2sa_truth=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)(PORT=20002)(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

## Making changes to listener.ora on one of the RAC node server (instance)

After SA installation is complete, the `listener.ora` file should point/link to the `listener.ora-operational` file.

In an Oracle RAC environment, only one of the RAC nodes or instances is used during installation/upgrade process. The SA Installer connects to only one Oracle instance to modify the Model Repository. During the normal SA operations, all the RAC nodes are used.

The SA Installer puts the database in a restricted mode during the Model Repository installation. The database is removed from the restricted mode after successful installation/upgrade of the Model Repository. When the database is in restricted mode, only certain privileged users are allowed to connect. To accommodate the remote truth installation process, two sets of `listener.ora` files are required on the SA server. The files can be given any name. By default the `listener.ora` files can be found in `$ORACLE_HOME/network/admin`.

`listener.ora-operational` – this copy of `tnames.ora` is used during normal SA operation.

You can use softlinks to point `listener.ora` to either `listener.ora.ora-install_upgrade` or `listener.ora.ora-operational`.

```
ln -s listener.ora-operational listener.ora.ora (before SA regular operations)
```

`listener.ora-operational` - this file is used to start the listener when SA is running in normal operational mode. Make a note of the text that is in **BOLD** letters.

```
# listener.ora.rac1pub Network Configuration File: /u01/app/asm/product/11.1.0/db_1/network/admin/listener.ora.rac1pub
# Generated by Oracle configuration tools.
```

```
LISTENER_RAC1PUB =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
      (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521)(IP = FIRST))
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.173.210)(PORT = 1521)(IP = FIRST))
    )
  )
```

```
SID_LIST_LISTENER_RAC1PUB =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /u01/app/oracle/product/11.1.0/db_2)
      (PROGRAM = extproc)
    )
  )
```

Use softlink to link the file to `listener.ora` file

```
ln -s listener.ora-operational listener.ora.ora
```

Ensure that you start the listener as follows:

```
> lsnrctl start LISTENER_RAC1PUB
```

## Vault.conf file changes

In an Oracle RAC environment, the `vault.conf` file must be modified after SA installation is complete. Modify `/etc/opt/opsware/vault/vault.conf` to specify the complete `tnsname` definition instead of the `SID`. For example:

- Before:

```
truth.sid: truth
```

- After:

```
truth.sid=(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST =
rac1-vip.dev.opsware.com)(PORT = 1521)) (ADDRESS = (PROTOCOL = TCP)
(HOST = rac2-vip.dev.opsware.com)(PORT = 1521)) (LOAD_BALANCE = yes)
(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = truth)
(FAILOVER_MODE = (TYPE = SELECT) (METHOD = Preconnect) (RETRIES = 180)
(DELAY = 5))))
truth.port: 1521
```

Restart the `vaultdaemon`:

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

## Upgrading the Model Repository

To upgrade the Model Repository in an Oracle RAC environment, follow the same procedure as [Installing the Model Repository](#) on page 126. If you are doing a remote database installation, then make sure that you modify your `listener.ora` is on one of the RAC instances and `tnsnames.ora` on the server where the SA Installer is run. It is recommended that you test the connection as suggested in section [Testing connection from SA machine to database](#) on page 131.

# Planning and Installation Guide, First Core Post-Installation Tasks (page 121)

The section below is incorrect:

---

## Edit the `jboss_wrapper.conf` File

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 SA 7.80 does not use Java 1.4.2, these lines are no longer required.

---

The correct instructions are:

You should adjust the values for `wrapper.java.additional.x` where `x > 8` is consecutive.

For example:

Change this:

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8
```

#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/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar
```

#Add location of keystore. This is used to make SSL request.

```
wrapper.java.additional.9=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore
```

# Bug 171948 - Need more PermGen

```
wrapper.java.additional.10=-XX:MaxPermSize=80m
```

To this:

```
wrapper.java.additional.1=-DTCMgmtEngine=1
wrapper.java.additional.2=-Duser.dir=/opt/NA750/server/ext/jboss/bin
wrapper.java.additional.3=-Xmn170m
wrapper.java.additional.4=-Djava.awt.headless=true
wrapper.java.additional.5=-Dfile.encoding=UTF8
```

#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/NA750/server/ext/wrapper/
lib/CORBA_1.4.2_13.jar
```

#Add location of keystore. This is used to make SSL request.

```
wrapper.java.additional.6=-Djavax.net.ssl.trustStore=/opt/NA750/server/ext/
jboss/server/default/conf/truecontrol.keystore
```

# Bug 171948 - Need more PermGen

```
wrapper.java.additional.7=-XX:MaxPermSize=80m
```





