

HP Server Automation

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

Software Version: 9.01

Release Notes

Document Release Date: September 2010
Software Release Date: September 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

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

This site requires that you register for an HP Passport and sign in.

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
	September 2010	Document Created.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

<https://ovrd.external.hp.com/rd/register>

To find more information about access levels, go to:

http://support.openview.hp.com/access_level.jsp

Contents

1	New in SA 9.01	15
	Critical Defect Fixes and Known Defects	15
	Supported Operating Systems	15
	New Supported Platforms: Managed Servers	15
	New Supported Platforms: Virtualization	16
	New Supported Platforms: Storage Visibility and Automation	16
	New Product Integration	16
	Support for Solaris Patch Bundles	17
	Detecting Benign Error Codes with Solaris Patching	17
	New Application Deployment Manager Features	17
	Just-In-Time Targets	17
	Bare Metal Provisioning	18
	Behavior When a Pre-Install Script Fails	18
	Approving Blocked Jobs that Run SA Extensions	18
	Restricting Access to RPM Folders	18
	Windows Server 2008 R2 Support	19
	Sunsolve Website Rebranding and the solpatch_import Script	19
	Red Hat Enterprise Linux 5.x PPC64 OS Provisioning	19
	Red Hat Enterprise Linux 5.x PPC64 Sample Kickstart File	19
	DHCP Configuration For PowerPC	20
	Network Booting Red Hat Enterprise Linux 5.x PPC64 Servers	20
	SE Connector/Storage Visibility and Automation	21
	New Features	21
	SE Connector Content	22
	Remediation	22
	Attaching and Remediating the SE Storage Scanner and SE Connector Update Policies	22
	Documentation for SA 9.01	23
2	Installing SA 9.01	25
	General Information	25
	Script Running Order	27
	Database Schema Update Procedure	27
	Patch Installation Procedure	29
	Software Repository Content Upgrade	30
	General Information	30
	Upgrading the First Core Content	30
	Rolling Back the Upgrade	30
	Rolling Back the Patch	30
	Rolling Back the Database Schema Update	31
	Post-Patch Installation Tasks	31
	Windows Server 2008 R2 x64	31
	Requirements	32

Running the Script	32
Effect on Software Policies	33
Effect on Packages	34
Effect Application Configurations	34
Effect on Patch Policies	34
Effect on OS Provisioning: MRLs, Installation Profiles and OS Sequences.	35
WindowsImageName Custom Attribute	35
The populate-opsware-update-library Script	35
Windows Server CLI Installation	35
3 Fixed in SA 9.01	37
AAA	37
QCCRID: 44941.	37
Agent.	37
QCCRID: 108132.	37
QCCRID: 111496.	37
QCCRID: 111807.	38
QCCRID: 111970.	38
QCCRID: 112564.	39
QCCRID: 113351.	39
QCCRID: 114142.	39
Application Configuration	39
QCCRID: 61445.	39
QCCRID: 70119.	40
QCCRID: 76553.	40
QCCRID: 80888.	40
QCCRID: 106203.	40
QCCRID: 111027.	41
QCCRID: 111558.	41
QCCRID: 111765.	41
QCCRID: 111819.	41
QCCRID: 111851.	42
QCCRID: 111992.	42
QCCRID: 112119.	42
QCCRID: 112121.	42
QCCRID: 113689.	43
QCCRID: 114041.	43
QCCRID: 114398.	43
Application Deployment Manager	43
QCCRID: 104590.	43
QCCRID: 107544.	44
QCCRID: 109343.	44
QCCRID: 110134.	44
QCCRID: 110852.	44
QCCRID: 110875.	45
QCCRID: 111038.	45
QCCRID: 111103, 111128.	45

QCCRID: 111121.....	45
QCCRID: 111218.....	46
QCCRID: 111223.....	46
QCCRID: 111236.....	46
QCCRID: 111325.....	46
QCCRID: 111398.....	47
QCCRID: 111500.....	47
QCCRID: 111507.....	47
QCCRID: 111595.....	47
QCCRID: 111656.....	48
QCCRID: 111680.....	48
QCCRID: 111681.....	48
QCCRID: 111926.....	48
QCCRID: 111959.....	49
QCCRID: 112013.....	49
QCCRID: 112597.....	49
QCCRID: 112941.....	49
QCCRID: 113127.....	50
QCCRID: 113283.....	50
QCCRID: 113342.....	50
QCCRID: 113382.....	50
QCCRID: 113426.....	51
QCCRID: 113491.....	51
QCCRID: 113603.....	51
QCCRID: 113785.....	51
QCCRID: 113283.....	52
QCCRID: 113841.....	52
QCCRID: 113897.....	52
QCCRID: 113911, 114664, 114856.....	52
QCCRID: 113965, 115706.....	53
QCCRID: 114197.....	53
QCCRID: 114666.....	53
QCCRID: 114764.....	54
QCCRID: 114918.....	54
QCCRID: 114921.....	54
QCCRID: 115117.....	54
QCCRID: 115184.....	55
QCCRID: 115204.....	55
QCCRID: 115209.....	55
QCCRID: 115367.....	55
QCCRID: 115368.....	56
QCCRID: 115534.....	56
QCCRID: 115546.....	56
QCCRID: 115949.....	56
Audit and Remediation.....	57
QCCRID: 81358.....	57
QCCRID: 105021.....	57

QCCRID: 105146	57
QCCRID: 108616	57
QCCRID: 110611	58
QCCRID: 110811	58
QCCRID: 111682	58
QCCRID: 111791	58
QCCRID: 113305	59
QCCRID: 116286	59
QCCRID: 116514	59
Extensible Discovery	59
QCCRID: 110987	59
Global File System	60
QCCRID: 110903	60
QCCRID: 112418	60
QCCRID: 112419	60
Installer	60
QCCRID: 76655	60
ISM Tool	61
QCCRID: 110511	61
QCCRID: 111304	61
QCCRID: 111662	61
Jobs and Sessions	62
QCCRID: 111800	62
QCCRID: 111802	62
QCCRID: 111856	62
Model Repository	62
QCCRID: 83813	62
QCCRID: 93757	63
OS Provisioning	63
QCCRID: 65480	63
QCCRID: 89108	64
QCCRID: 93881	64
QCCRID: 95401	64
QCCRID: 109925	65
QCCRID: 111245	65
QCCRID: 111445	65
QCCRID: 111845	65
QCCRID: 113004	66
QCCRID: 113056	66
QCCRID: 114303	66
QCCRID: 114403	66
QCCRID: 103377	67
QCCRID: 107141	67
QCCRID: 110077	67
Patch Management	67
QCCRID: 92124	67
Patch Management for Solaris	68

QCCRID: 110313.....	68
QCCRID: 112588.....	68
QCCRID: 113591.....	68
Patch Management for Unix.....	68
QCCRID: 110273.....	68
Patch Management for Windows.....	69
QCCRID: 111964.....	69
QCCRID: 110340.....	69
QCCRID: 110391.....	69
QCCRID: 111862.....	70
QCCRID: 114337.....	70
SA Client.....	70
QCCRID: 81123.....	70
QCCRID: 91685.....	70
SA-OO Integration.....	71
QCCRID: 111738.....	71
QCCRID: 111740.....	71
QCCRID: 112466.....	71
SAS Web Client.....	72
QCCRID: 111394.....	72
QCCRID: 114769.....	72
Server Automation Visualizer.....	72
QCCRID: 94138.....	72
QCCRID: 110100.....	72
Server Module.....	73
QCCRID: 88807.....	73
QCCRID: 91597.....	73
QCCRID: 107867.....	73
QCCRID: 111503.....	73
QCCRID: 111521.....	74
QCCRID: 112489.....	74
QCCRID: 112529.....	74
QCCRID: 113052.....	74
QCCRID: 113804.....	75
Software Management.....	75
QCCRID: 112589.....	75
QCCRID: 112702.....	75
QCCRID: 114781.....	75
QCCRID: 111793.....	76
QCCRID: 111861.....	76
SE Connector.....	76
QCCRID 93313.....	76
QCCRID 93316.....	77
Storage Host Agent Extension.....	77
QCCRID 100922.....	77
QCCRID 101464.....	77
Virtual Center.....	78

QCCR1D: 109849	78
QCCR1D: 109887	78
QCCR1D: 111780	78
QCCR1D: 115353	78
QCCR1D: 113887	78
QCCR1D: 113891	79
Virtualization	79
QCCR1D: 71640	79
QCCRID: 71995	79
QCCRID: 77903	80
QCCRID: 78017	80
QCCRID: 81233	80
QCCRID: 81241	80
QCCRID: 92213	80
QCCRID: 92216	81
QCCRID: 92336	81
QCCRID: 93224	81
QCCRID: 93612	81
QCCRID: 93686	82
QCCRID: 93713	82
QCCRID: 93764	82
QCCRID: 104418	82
QCCRID: 105257	83
QCCRID: 108705	83
QCCRID: 109849	83
QCCRID: 109874	83
QCCRID: 110481	84
QCCRID: 111307	84
QCCRID: 111363	84
QCCRID: 111775	84
QCCRID: 111847	84
QCCRID: 111922	85
QCCRID: 111972	85
QCCRID: 112176	85
QCCRID: 112376	85
QCCRID: 112417	86
QCCRID: 112431	86
QCCRID: 112733	86
QCCRID: 113607	86
QCCRID: 113659	87
QCCRID: 111590	87
QCCRID: 111691	87
Other	87
QCCRID: 109998	87
QCCRID: 112878	88
4 Known Problems, Restrictions, and Workarounds in SA 9.01	89
Agent Installer	89

QCCRID: 107917.....	89
QCCRID: 111593.....	89
Agents.....	90
QCCRID 100660.....	90
QCCRID: 110347.....	90
Application Configuration.....	91
QCCRID: 50099.....	91
QCCRID: 111765.....	91
Application Deployment Manager.....	91
QCCRID: 110220.....	91
QCCRID: 110637.....	92
QCCRID: 111106.....	92
QCCRID: 111925.....	92
QCCRID: 113202.....	92
QCCRID: 115187.....	93
Audit and Remediation.....	94
QCCRID: 102706.....	94
BSA Essentials Dataminer.....	94
QCCRID: 112784.....	94
Database Scanner for Oracle.....	95
QCCRID 88091.....	95
QCCRID 91143.....	95
QCCRID 93690.....	95
Bug ID: 156909 / QCCRID 68263.....	96
Installer.....	96
QCCRID 100931.....	96
QCCRID 114639.....	97
ISM Tool.....	97
QCCRID: 110511.....	97
Model Repository.....	98
QCCRID: 83813.....	98
QCCRID: 113314.....	98
OS Provisioning.....	99
QCCRID: 100928.....	99
QCCRID 102830.....	99
QCCRID: 103362.....	100
QCCRID: 103394.....	100
QCCRID: 103602.....	100
QCCRID: 104194.....	100
QCCRID: 104739.....	101
QCCRID: 109044.....	101
QCCRID: 109077.....	101
QCCRID: 110563.....	101
QCCRID: 111245.....	102
QCCRID: 111337.....	102
QCCRID: 111445.....	102
QCCRID: 114523.....	102

QCCRID: 111781.....	103
QCCRID: 111845.....	103
QCCRID: 115063.....	103
QCCRID: 116936.....	104
Patch Management for Solaris	104
QCCRID: 98409.....	104
QCCRID: 100566.....	104
QCCRID: 109142 and 115536	105
QCCRID: 109359 and 109361	105
QCCRID: 111342.....	106
QCCRID: 114156.....	106
Patch Management for Windows.....	107
QCCRID: 102713.....	107
QCCRID: 108451.....	107
QCCRID: 105098.....	107
QCCRID: 110257.....	108
QCCRID: 110471.....	108
QCCRID: 111397.....	109
SA Client (Framework)	109
QCCRID:105671	109
SA Client (Search)	109
Bug ID: 155094 / QCCRID 66448.....	109
SA/NA Integration	110
QCCRID:90653	110
SA/OO Integration	110
QCCRID:102614	110
SA/SAR Reports	111
QCCRID: 105234.....	111
QCCRID: 107293.....	111
QCCRID: 112434.....	112
SAS Web Client	113
QCCRID: 109000.....	113
Satellites.....	113
QCCRID: 97659.....	113
Script Execution.....	114
QCCRID: 79545.....	114
SE Connector	114
QCCRID 88755	114
QCCRID 91582	114
QCCRID 105778	115
Server Automation Installer	115
QCCRID: 111215.....	115
Software Management.....	115
QCCRID: 100754.....	115
QCCRID: 101517.....	116
QCCRID: 102564.....	116

QCCRID: 102934	117
QCCRID: 111356	117
QCCRID: 115665	117
Storage Host Agent Extension	117
QCCRID 93630	117
QCCRID 105382	118
QCCRID 105953	118
QCCRID 106400	118
QCCRID 106699	119
QCCRID: 107944	119
QCCRID 109306	119
QCCRID 111724	119
QCCRID 111727	120
QCCRID 116264	120
QCCRID 116775	121
Bug ID: 149406 / QCCRID 60760	121
Bug ID: 149707 / QCCRID 61061	121
Bug ID: 151921 / QCCRID 63275	121
Bug ID: 152016 / QCCRID 63370	122
Bug ID: 152942 / QCCRID 64296	122
Bug ID: 154418 / QCCRID 65772	122
Bug ID: 154971 / QCCRID 66325	123
Bug ID: 155476 / QCCRID 66830	123
Bug ID: 157044 / QCCRID 68398	123
Bug ID: 157579 / QCCRID 68933	123
Bug ID: 158923 / QCCRID 70277	124
Bug ID: 159156 / QCCRID 70510	124
Bug ID: 159580 / QCCRID 70934	124
Bug ID: 164951 / QCCRID 76305	125
Bug ID: 168716 / QCCRID 80070	125
Bug ID:168889 / QCCRID 80243	125
Bug ID: 167103 / QCCRID 78457	125
Virtualization	126
QCCRID: 90019	126
QCCRID: 106085	126
QCCRID: 104418	127
QCCRID: 105999	127
QCCRID: 106909	127
QCCRID: 109887	127
QCCRID: 110035	128
QCCRID: 111307	128
QCCRID: 111789	128
QCCRID: 111922	128
QCCRID: 111972	129
QCCRID: 116276	129
QCCRID: 116983	130
Web Services Data Access Engine	130

QCCRID: 111039.....	130
QCCRID: 112222.....	130
5 Documentation Errata.....	133
Application Deployment Manager Context-sensitive (F1) Help.....	133
SA 9.0 Single-Host Installation Guide.....	133
Create a User Account with Administrator Privileges (Page 15).....	133
SA 9.0 Simple/Advanced Installation Guide.....	134
SA 9.0 Simple/Advanced Installation Guide and Oracle Setup for the Model Repository.....	135
SA 9.0 Simple/Advanced Installation Guide and Oracle Setup for the Model Repository.....	136
Upgrading SA to Version 9.0 in a Oracle RAC Environment.....	136
Requirements.....	136
Pre-upgrade Tasks.....	136
During the Upgrade.....	136
Post-upgrade Tasks.....	137
Adding a Secondary Core Using the SA 9.0 Installer in an Oracle RAC or Remote Database Environment.....	138
Exporting Model Repository Content.....	138
Adding the Secondary Core that Uses Oracle RAC or a Remote Database.....	139
Model Repository Pre-installation Tasks.....	139
After Model Repository Installation.....	140
After Installation is Complete.....	140
Storage Visibility and Automation User Guide.....	141
Storage Visibility and Automation Installation & Administration Guide.....	141

1 New in SA 9.01

This document includes release note information for Server Automation, Storage Visibility and Automation, and SE Connector.



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

Critical Defect Fixes and Known Defects

Critical defect fixes and known defects each have their own chapters: [Fixed in SA 9.01](#) on page 37 and [Known Problems, Restrictions, and Workarounds in SA 9.01](#) on page 89. Within those chapters, defects are conveniently listed alphabetically by subsystem, and then numerically under each subsystem.

Supported Operating Systems

For a list of supported platforms for Server Automation 9.01 Cores, Agents, clients, and Satellites, see the *Server Automation Compatibility Matrix*.

For a list of supported platforms for Storage Visibility and Automation 9.01 Managed Servers, SE Connector, SAN Arrays, Fibre Channel Adapters, SAN Switches, File System Software, Database Support, and Storage Essentials Compatibility, see the *Storage Visibility and Automation Compatibility Matrix*.



To check for updates to these documents, go to <http://support.openview.hp.com/selfsolve/manuals>. The HP Software Product Manuals site requires that you register for an HP Passport and sign in. To register for an HP Passport, select the **New users - please register** link on the HP Passport login page.

New Supported Platforms: Managed Servers

- CentOS 5.4 – x64, i386
- CentOS 5.5 (i386, x64)
- Novell OES2 SP2 (i386, x64)

- Oracle Enterprise Linux 4.8, 5.4 x64, i386
- Oracle Enterprise Linux 5.5 (i386, x64)
- Red Hat Enterprise Linux 4 Update 8 x64, i386, IA64
- Red Hat Enterprise Linux 5.4 IA64
- Red Hat Enterprise Linux 5.4, 5.3, 5.2 POWER **
- Red Hat Enterprise Linux 5.5 x64,i386,Power,IA64
- Solaris 10 U8 – SPARC, x64
- SUSE Linux Enterprise Server 10 SP3 x64, i386
- SUSE Linux Enterprise Server 10 SP 3, 11 POWER
- VMware ESX4.0 U1, ESXi 4.0 U1, ESX 3.5 U5, ESXi 3.5 U5

** Requires a modified OS Provisioning process. See [Red Hat Enterprise Linux 5.x PPC64 OS Provisioning](#) on page 19.

New Supported Platforms: Virtualization

- Japanese Windows 2008 x64 Hyper-V
- Windows R2 x64 Hyper-V
- VMware ESX 3.5 U5, ESXi 3.5 U5
- VMware ESX 4 u1 / ESXi 4 u1

New Supported Platforms: Storage Visibility and Automation

- CentOS 5.4-5.5 x64, i386
- Oracle Enterprise Linux 4.8, 5.4 x64, i386
- Red Hat Enterprise Linux 4 Update 8 x32, x64, IA64
- Red Hat Enterprise Linux 5.4 (Advanced) x32
- Red Hat Enterprise Linux 5.5 x64, i386, IA64
- Solaris 10 U8 SPARC, x64
- SUSE Linux Enterprise Server 10 SP3 x32, x64
- Windows Server 2008 SP2 x32, x64
- Windows Server 2008 R2 x64
- VMware ESX 3.5 U5

New Product Integration

- Network Automation (NA) 7.50, 7.60, 9.0

- Orchestration Automation 9.0, 7.60, 7.51

Support for Solaris Patch Bundles

This SA release 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 install Solaris patch bundles directly on managed servers or use Solaris patch policies to install the patch bundles. For more information, see “Patch Management for Solaris” in the *SA User Guide: Application Automation*.

Detecting Benign Error Codes with Solaris Patching

SA can now detect benign error codes when installing Solaris patches. 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. SA detects these benign error codes and reports success in most cases. For more information, see “Patch Management for Solaris” in the *SA User Guide: Application Automation*.

New Application Deployment Manager Features

The following new features are now available in the Application Deployment Manager.

Just-In-Time Targets

In SA release 9.01, the Application Deployment Manager introduces Just-In-Time (JIT) targets. Targets can now be provisioned dynamically by way of an HP Operations Orchestration (OO) flow. This enables you to assemble targets (at deployment time) with servers from varied sources such as the cloud, hypervisors, and resource scheduling software suites.

Simply create an OO flow that automates the process of selecting servers using the technology that makes sense in your environment. After the OO flow is configured, the Application Deployment Manager prompts (at deployment time) for the number of servers to be used in each tier. It then passes this information into the OO flow, which chooses the individual servers. JIT targets can later be re-used just as if they had been created using the Application Deployment Manager Target Editor. Existing targets can even be used as templates—a copy is made with the same set of tiers, and then servers are chosen by the OO flow.

For more information, refer to “Just-In-Time Targets” in the *Application Deployment Manager User Guide*.

Bare Metal Provisioning

In SA release 9.01, the Application Deployment Manager introduces bare metal provisioning for application deployment. Using bare metal provisioning, it is now possible to automate application deployment from raw hardware to running software.

Bare metal provisioning works in a manner similar to middleware provisioning in SA release 9.0. For each Application Deployment Manager tier, it is now possible to specify an HP Server Automation OS Sequence. The specified OS Sequence will be applied only when application deployment targets contain unprovisioned servers. This can be very useful when adding capacity for a particular application—simply add new (unprovisioned) servers to a target and redeploy.

For more information, refer to “Provisioning Servers at Deployment Time” in the *Application Deployment Manager User Guide*.

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.

Before SA 9.01, 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 9.01, 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 9.01 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 9.01 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 Guide*.

Restricting Access to RPM Folders

In SA 9.01, 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.

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*.

Windows Server 2008 R2 Support

This release adds support for Windows Server 2008 R2. If you plan to provision or manage Windows Server 2008 R2 hosts, there are certain additional steps you must take during the patch installation process to ensure full compatibility and support for existing configurations (application configuration, software policies, and so on). See [Chapter 2, Windows Server 2008 R2 x64](#), on page 31 of this guide.

Sunsolve Website Rebranding and the solpatch_import Script

Oracle Corp. has rebranded the Sunsolve website therefore, before running `solpatch_import-action=create_db` as described in the *SA User Guide: Server Automation*, you must log in to your Sunsolve account and subscribe to patch download automation. For more information, see:

<http://support.openview.hp.com/selfsolve/document/KM961930>

Red Hat Enterprise Linux 5.x PPC64 OS Provisioning

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

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

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 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
```

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

6 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.

- 7 The Red Hat Anaconda installer starts. If your server has multiple network interfaces, the installer may prompt you to specify the interface to use.
- 8 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.
- 9 (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.
- 10 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*.

SE Connector/Storage Visibility and Automation

New Features

- Unreplicated LUN count audit
- Storage Device Replication Data
 - EMC (SRDF/TimeFinder)
 - Hitachi Replication
 - HP EVA, XP Replication
 - NetApp Snapshots & Sync Mirror
- Support for SE 6.2.1 and SE 6.3
- Co-existence of support for Storage Essentials Central Management System (CMS) versions 6.11, 6.2, 6.2.1, and 6.3
- Content changes (See [SE Connector Content](#) on page 22.)

It is no longer necessary to install the SE Connector updates through BSAEN. The updates are installed on the SA core when you install the 9.01 SA patch.

SE Connector Content

The following content (which will be installed when you install the patch) was added to the patch uploader for the SE Connector:

Content	Description
SE Storage Scanner	Full SE Connector with SE Client Libraries from versions 6.1.1, 6.2, 6.2.1 and 6.3
SE Connector Update for 6.1.1	SE 6.1.1 Client Libraries
SE Connector Update for 6.2	SE 6.2 Client Libraries
SE Connector Update for 6.2.1	SE 6.2.1 Client Libraries
SE Connector Update for 6.3	SE 6.3 Client Libraries

Remediation

The following mandatory remediation functionality was added to SE Connector:

To Communicate With This CMS	Remediate with This
SE 6.1.1	SE Storage Scanner policy (base policy with 6.1.1 SE client libraries)
SE 6.2	SE Storage Scanner policy, then with the SE Connector update for 6.2.0 policy
SE 6.2.1	SE Storage Scanner policy, then with the SE Connector update for 6.2.1 policy
SE 6.3	SE Storage Scanner policy, then with the SE Connector update for 6.3 policy

Attaching and Remediating the SE Storage Scanner and SE Connector Update Policies

This section describes the steps to follow when you attach and remediate the SE Storage Scanner and SE Connector Update policies.

To attach and remediate:

- 1 Attach the software policy SE Storage Scanner to the managed server.
- 2 Remediate the server.
- 3 If your HP Storage Essentials management server is version 6.1.1, you do not need to follow any more steps.
- 4 If the HP Storage Essentials management server is version 6.2 or later, attach the software policy SE Connector Update for your version to the managed server.

The version of the SE Connector Update must be compatible with the version of the Storage Essentials server, which means that the version numbers of the SE Connector Update libraries must be the same as the version of the Storage Essentials. For example, if you have SE 6.2, installed, you will have to install the SE Storage Scanner first, then install the SE Connector Update for 6.2.

Documentation for SA 9.01

The following documentation is provided with this patch release:

- *Server Automation Release Notes*
- *Server Automation Critical Fixes*
- *Server Automation Install Procedures*
- *Server Automation Compatibility Matrix*
- *Storage Visibility and Automation Compatibility Matrix*

The following SA 9.01 documentation has been updated for this patch release:

- *Online Help* (Updated!)
- *SA Policy Setter Guide* (Updated!)
- *SA User Guide: Application Automation* (Updated!)
- *SA User Guide: Application Deployment* (Updated!)
- *SA User Guide: Server Automation* (Updated!)

The following SA 9.0 documentation is still valid for this patch release:

- *SA Overview and Architecture Guide*
- *SA Single-Host Installation Guide*
- *SA Simple / Advanced Installation Guide*
- *SA Upgrade Guide*
- *SA Quick Reference: SA Installation*
- *SA Oracle Setup for the Model Repository*
- *SA Administration Guide*
- *SA Integration Guide*
- *SA Content Utilities Guide*
- *SA Content Migration Guide*
- *SA Platform Developer Guide*
- *SA Application Configuration User Guide*
- *SA 9.0 and BSA Essentials 2.0 Reports*
- *Storage Visibility and Automation Installation & Administration Guide*
- *Storage Visibility and Automation Upgrade Guide*
- *Storage Visibility and Automation User Guide*

- *Storage Visibility and Automation Compatibility Matrix*
- *Storage Compliance User Guide*
- *Storage Reports User Guide*
- *SE Connector Installation Guide*
- *Technical Note: EMC VCMDB and Gatekeeper Devices Have Incomplete Storage Supply Chain*



To check for updates to these documents, go to <http://support.openview.hp.com/selfsolve/manuals>. The HP Software Products Manual site requires that you register for an HP Passport and sign in. To register for an HP Passport, select the **New users - please register** link on the HP Passport login page.

2 Installing SA 9.01

This section describes the SA 9.01 installation procedure.



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

General Information

- SA 9.01 can be rolled back, but only to the previous full release, SA 9.0.
- The `patch_opsware.sh` script is used both for installing and for uninstalling SA 9.01.
- There's no need to supply a response file with `patch_opsware.sh`.
- The `patch_database.sh` script is used both for installing and rolling back database schema changes required for SA 9.01.
- You must run the `patch_database.sh` script on all Model Repository hosts in the First Core and all Secondary Cores. Note that the Oracle database can exist on a different host than the Model Repository host.
- The response file used to last install/upgrade of the SA Core must be supplied when invoking `patch_database.sh`.
- This patch includes updated Server Agents that are uploaded to the Software Repository. However, no agents are upgraded on core machines (in the Model Repository) or on Managed Servers without manual intervention
- SA 9.01 can only be installed on systems running SA versions with a Build ID of **opsware_40.0.2538.***.

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_40.0.2538.*
```

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_40.0.xxxx.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 terminates.
- 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 9.01 or higher) than the secondary cores.

If you must roll back the SA 9.01 patch in a Multi-master Mesh, HP recommends that you roll back the secondary cores and satellites first, then the primary core.

- Mixed version core environments are not supported. However, during the patch upgrade, a transitory mixed core version environment is supported. For example, while the patch upgrade is in progress, cores at different patch levels can temporarily coexist in a Multimaster Mesh.
- 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 fails 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 fails 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.

Script Running Order

The patch install scripts must be run in the following order:

Table 1 SA 9.01 Script Running Order

Upgrade From	To	Script Running Order
9.0	9.01	1 patch_database.sh 2 patch_opsware.sh 3 patch_contents.sh
Rollback From	To	
9.01	9.0	1 patch_opsware.sh 2 patch_database.sh

Database Schema Update Procedure

The script run during this procedure makes required changes to the Model Repository including adding required tables and objects. Perform the following tasks to install SA 9.01 database updates:

- 1 Before running the patch install script, perform steps below to ensure that the script `20_truth_modify_truth_stats_job_90.sh` script is run during patch installation.

This script modifies the TRUTH database users `dba_job` that collects schema statistics.



This is an optional script that fixes issues described in QCR1D: 93757. This script is run by the patch install script, `patch_database.sh`, only when you have made the following changes.

- a Create the file:

```
/var/opt/opsware/OPSWpatch_sql/optional_updates.conf
```

on the server on which you will run the patch install script, `patch_database.sh`.

- b Edit `optional_updates.conf` and add this entry:

```
truth_modify_truth_stats_job=1
```

When you run the patch install script `patch_database.sh`, it checks for the existence of `optional_updates.conf`, and if the file exists and contains the entry specified in step b, it runs the script `20_truth_modify_truth_stats_job_90.sh` which then modifies the `dba_job` that collects schema statistics.

If `optional_updates.conf` is not found, or if the `truth_modify_truth_stats_job=1` entry is not found in the file, then the script `20_truth_modify_truth_stats_job_90.sh` is not executed.

- 2 Mount the SA 9.01 distribution. Invoke `patch_database.sh` on the Model Repository host:

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

Where `<response file>` is the response file last used to install/upgrade the system.

Usage: `patch_database.sh [--verbose] -r <response file>`

`patch_database.sh` automatically detects if a database update is already installed and presents a corresponding menu:

- a If the database update has not been previously applied, you see the following:

```
Welcome to the Opsware Installer.
It appears that you do not have a database update installed on this
system.
Press 'i' to proceed with patch installation.
Press 's' to show patch contents.
Press 'q' to quit.
Selection: i
```

Enter `i` at the prompt to begin the database update.

- b If the database update has previously been applied, you see the following:

```
Welcome to the Opsware Installer.
It appears that you have installed or attempted to install a previous
version of the database update 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: u
You chose to upgrade the patch. Continue? [y/n]: y
```

Enter `u` at the prompt then `Y` to begin the database update.

- 3 After you make your selection, the installer completes the new (or interrupted) installation. On completion, you see a screen similar to the following:

```
[timestamp] Done with component Opsware SQL patches.
[timestamp] #####
[timestamp] Opsware Installer ran successfully.
[timestamp] #####
```



After running the `patch_database.sh` script, 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, role_class_bridge.
```

This error is invalid and you can disregard it.

Patch Installation Procedure



Before performing the tasks in this section ensure that you have completed the tasks listed in [Database Schema Update Procedure](#) on page 27.

Perform the following tasks to install SA 9.01:

- 1 Mount the SA 9.01 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: i
```

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: u
```

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 only updates 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 is automatically 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.
```

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

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

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

Rolling Back the Upgrade

Rolling Back the Patch

To rollback SA 9.01 to SA 9.0, invoke the script:

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

If this is a patched system, the following is 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 9.01 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 are retained. If you try to install these patches or attach the policies, an error will occur.
- Rolling back SA 9.01 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 the Database Schema Update



If you created the optional file `/var/opt/opsware/OPSWpatch_sql/optional_updates.conf` with the entry `truth_modify_truth_stats_job=1` (modifies the TRUTH database users `dba_job` that collects schema statistics.) during the install process as described [step 1](#) on page 27, you must ensure that the same `optional_updates.conf` file is available during the rollback process.

To roll back the database schema update, enter this command:

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

Where `<response file>` is the response file last used to install/upgrade the system.

If the database has been updated, you see the following:

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

Enter `r` at the prompt to begin the database schema update rollback.

Post-Patch Installation Tasks

Windows Server 2008 R2 x64

SA 9.01 and later provides improved support for Windows Server 2008 R2 x64. Windows Server 2008 R2 x64 now appears with its own entries in the SA Client rather than as a subset of Windows Server 2008.

However, there are some tasks you must perform in order to migrate any Software Policies, Application Configurations, packages (units), Patch Policies and/or OS Provisioning objects you may already have set up for your server(s).

Requirements

- You must run the script on the Core's Software Repository (`word`) host.
- You must run the script on a machine that has `OPSWpytwist` installed.
- You must run the script on an active core, all SA Core Components must be running.
- You must run the script as `root`.
- You must log in to the SA Client and navigate to **Administration > Patch Settings > Windows Patch Downloads > Patch Products**. Use the Edit button and add the Windows Server 2008 R2 x64 option.
- You must re-import the latest MBSA patch database by selecting Patch Database, then the Import from Vendor button.
- If your Hyper-V servers are installed with Windows Server 2008 R2 x64, you must either run hardware registration manually or wait for the scheduled hardware registration to complete before you run:
 - Data Reload on the Hyper-V server
 - Create VM, Modify VM, Delete VM, or any control operation on a Hyper-V VM

Running the Script

You run the script, `windows_2008_R2_fix_script.pyc`, provided with SA 9.01 and later which is found in the directory:

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

The script is invoked as follows:

```
/opt/opsware/bin/python2 windows_2008_R2_fix_script.pyc [--mrl=<MRL_ID>|--listmrls|--help
```

- 1 To migrate a core's Windows Server 2008 R2 x64 servers, invoke the script without arguments on the Software Repository host.

```
/opt/opsware/bin/python2 windows_2008_R2_fix_script.pyc
```

- 2 After the server(s) are migrated, invoke the script with the `--listmrls` option which provides a list of MRLs indicating OS Sequences that must be migrated.

```
/opt/opsware/bin/python2 windows_2008_R2_fix_script.pyc --listmrls
```

- 3 Note the MRLs from the previous step and invoke the script with the `--mrl=<MRL_ID>` option to migrate any OS Sequences with attached Patch Policies or Software Policies.



It is very important that you ensure that the MRL(s) specified when you invoke this migration script with the `--mrl=<MRL_ID>` option are correct. Once the script is invoked, migration begins immediately. Providing the incorrect information when invoking this script can cause irreversible data integrity errors.

The script has the following options:

Table 2 Windows Server 2008 R2 Migration Script Options

Options	Description
<code>--listmrls, -l</code>	List all Windows Server 2008 x64 MRLs (ID, Name and Media Path)
<code>--MRL=<MRL ID></code>	Migrate the MRL with the specified ID to the Windows Server 2008 R2 x64 platform. Can be specified multiple times.
<code>--help, -h</code>	Display usage and help



Migrated objects other than Patch Policies are not copied, they are attached to the new Windows Server 2008 R2 x64 configuration.

For Patch Policies, Windows Server 2008 R2 x64 copies are created of Windows Server 2008 x64 Patch Policies containing R2 patches (x64 patch library).

The Windows Server 2008 x64 Patch Policies are then detached from the Windows Server 2008 R2 x64 servers and the equivalent Windows Server 2008 R2 x64 Patch Policy copies are attached to the Windows Server 2008 R2 x64 servers.



You can run `windows_2008_r2_fix_script.py` multiple times without issue. The changes made by the script cannot be rolled back.

Effect on Software Policies

After migration completes, the Software Policy appears in the SA Client Navigation pane under Library/By Type/Software Policies/Windows/Windows Server 2008 R2 x64 and Windows Server 2008 x64.

During migration, Software Policies are modified only if:

- The software policy is attached to a Windows Server 2008 R2 x64 server and the software policy platform list contains Windows Server 2008 x64, or
- The Software Policy is attached to a device group, the device group contains a Windows Server 2008 R2 x64 server and the software policy platform list contains Windows Server 2008 x64.

When processing policy items the script looks for the following types of objects:

- Nested Software Policies
- Units (Packages)
- Application Configurations

If the script finds a policy item that has Windows Server 2008 x64 in the platform list it migrates that policy item to Windows Server 2008 R2 x64.

The order of items in the Software Policy is retained and remediation status remains unchanged.

If the script identifies an existing Software Policy as a Windows Server 2008 R2 x64 policy, it does not modify it during processing.

Effect on Packages

The script migrates only the packages that have Windows Server 2008 x64 in the platform list and are included as policy item inside a Software Policy that is migrated by the script.

After migration, the package appears in the SA Client under both the Windows Server 2008 x64 and Windows Server 2008 R2 x64 folders in Library/By Type/Packages/Windows.

The script does not take into account the package type. It looks for packages included in migrated Software Policies that are attached to Windows Server 2008 x64. Server Module Result objects, Windows Registry objects and Windows Services objects cannot be migrated by the script because their platform associations cannot be changed.

Properties settings (including general, archived scripts, install parameters, install scripts, uninstall parameters, uninstall scripts) are preserved.

Effect Application Configurations

The migration script migrates an application configuration if:

- It is attached to a Windows Server 2008 R2 x64 server and has Windows Server 2008 x64 in the platform list, or
- It is attached to a device group that contains a Windows Server 2008 R2 x64 server and has Windows Server 2008 x64 in the platform list, or
- It has Windows Server 2008 x64 in the platform list and is a policy item of a Software Policy that is migrated.

During migration the script adds Windows Server 2008 R2 x64 to the application configuration's platform list. The script also inspects all application configurations' associated templates (CML templates) and if a template has Windows Server 2008 x64 in the platform list it is also migrated.

There is no undo option.

Effect on Patch Policies

During migration, the script appends R2 to the Patch Policy name. For example, for a patch policy named 2008 XYZ Policy, the migration script creates a new Windows Server 2008 R2 x64 policy named 2008 XYZ Policy R2 if:

- There are Windows Server 2008 R2 x64 patches in 2008 XYZ Policy.
- There does not exist any patch policy named 2008 XYZ Policy R2 that contains patches applicable to platforms other than Windows Server 2008 R2 x64.



If a Windows Server 2008 R2 x64 policy named 2008 XYZ Policy R2 already exists, the applicable patches are added to it.

If Windows Server 2008 R2 x64 servers, or device groups containing Windows Server 2008 R2 x64 servers, are attached to Windows Server 2008 x64 patch policies, the migration script detaches these policies and attaches the newly created or updated equivalent Windows Server 2008 R2 x64 policies. Applicable Patch Policy exceptions are also migrated.

If metadata associated with Windows Server 2008 R2 x64 patches has been modified (for example, install/uninstall flags, pre/post install/uninstall scripts), that metadata are migrated.

Effect on OS Provisioning: MRLs, Installation Profiles and OS Sequences

To migrate OS Provisioning MRLs, Installation Profiles and OS Sequences, you must specify the MRL(s) to migrate by using the `--MRL=<MRL ID>` argument when invoking the migration script. You use the `--listmrls, -l` argument to display a list of all available Windows Server 2008 x64 MRLs to be migrated to Windows Server 2008 R2 x64. The list includes the MRL IDs, Names, and Media Paths.

All OS Installation Profiles and OS Sequences associated with a specified MRL are migrated to the Windows Server 2008 R2 x64 platform.



If you use dynamic MRLs (for example, the MRL path has script weaver tokens like `@mediaserver@`), the migration script cannot migrate the MRLs because they cannot be mounted. You can temporarily specify a full URL in the MRL using the SA Client interface before running the migration script. You can then restore the dynamic MRL specification after migration if needed.

WindowsImageName Custom Attribute

The specification of the `WindowsImageName` custom attribute with Windows Server 2008 R2 x64 is somewhat different from other platforms.

For Windows Server 2008 R2 x64, the expected values are:

```
Windows Server 2008 R2 SERVERDATACENTER
Windows Server 2008 R2 SERVERDATACENTERCORE
Windows Server 2008 R2 SERVERENTERPRISE
Windows Server 2008 R2 SERVERENTERPRISECORE
Windows Server 2008 R2 SERVERSTANDARD
Windows Server 2008 R2 SERVERSTANDARDCORE
Windows Server 2008 R2 SERVERWEB
Windows Server 2008 R2 SERVERWEBCORE
```

The populate-opsware-update-library Script

A new option, `--no_w2k8r2`, is provided for the `populate-opsware-update-library` script and is used to specify that Windows Server 2008 R2 x64 patch binaries should not be uploaded. For more information about the `populate-opsware-update-library` script, see the *SA User's Guide: Application Automation*.

Windows Server CLI Installation

If you plan to install the SA Command-line Interface (OCLI) on a Windows Server after upgrade to SA 9.01, 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 9.01

AAA

QCCRID: 44941

Description: SearchService.getObjRefs is returning non-readable object refs.

Platform: Independent

Subsystem: AAA

Symptom: For AAA ResourceType (OS_SEQUENCE), the SearchService.getObjRefs UAPI method is producing an AccessDenied Exception instead of returning a collection of objrefs where non-readable data is filtered out.

Resolution: Fixed.

Agent

QCCRID: 108132

Description: The Add Hypervisor action fails without providing useful error information.

Platform: Windows

Subsystem: Agent Deployment - Upgrade UI

Symptom: The Add Hypervisor Progress window displays an error message indicating that the job is completed and that the status of the job is failed.

Resolution: Fixed.

QCCRID: 111496

Description: Dormant Agent fails to connect to a core.

Platform: Unix, Windows

Subsystem: Agent Installer

Symptom: The Agent fails to start if the Agent Installer was unable to contact the core and download crypto. If the Agent starts and the network connection is restored, the Agent is still unable to connect with the core.

Resolution: Fixed.

QCCRID: 111807

Description: An SA-run UNIX script containing variables does not return the same values.

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

Subsystem: Agent

Symptom: A Unix script with environment variables, which is run by SA, does not return the same values that run on the managed server.

Resolution: Fixed. This fix supports the following UNIX environment:

HOME: users home directory

LOGNAME: users login name

USER: same as LOGNAME

TZ: time zone (not supported on Linux)

PATH: (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)

Valid PATH values are:

- 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. If you want to have your .profile (or any other script) executed, you must explicitly specify this in the sh script.

QCCRID: 111970

Description: Agent Tools Python Opsware API Access fails to install on VMware ESX servers.

Platform: VMware

Subsystem: Agent Tools

Symptom: There are ZIP errors when remediating a Python Opsware API Access policy.

Resolution: Fixed.

QCCRID: 112564

Description: Agent Install fails because of an Agent Gateway check fail.

Platform: Windows

Subsystem: Agent Installer

Symptom: The SA Agent will fail to install if there are minor delays in initializing the network interfaces when Windows is booted for the first time.

Resolution: Fixed.

QCCRID: 113351

Description: Windows Server 2008 R2 does not display an OS Version in the server record.

Platform: Windows Server 2008 R2

Subsystem: Agent

Symptom: SA does not display Windows Server 2008 R2 as OS version in the server record.

Resolution: Fixed.

QCCRID: 114142

Description: Discrepancy between `cpu_family` reported by different Agents on the same hardware.

Platform: Linux

Subsystem: Agent

Symptom: Unlike Windows, the `cpu_family` name reported by the Agent on Linux does not distinguish between 32bit (x86) and 64bit (x64) cpu family names.

Resolution: Fixed.

Application Configuration

QCCRID: 61445

Description: Need improved CML parsing error messages.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: When parsing or applying CML templates, the parser exceptions are not helpful. One error included the error message "Error on line: Null".

Resolution: Fixed.

QCCRID: 70119

Description: In the value set editor for the XML template, **Save Changes** expands all nodes.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: When you click **Save**, the state of the editor will be lost and all nodes will be expanded.

Resolution: Fixed.

QCCRID: 76553

Description: The Undo action for the Configuration Template properties Content tab does not work.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: The Undo action was not working for the Content tab.

Resolution: Fixed.

QCCRID: 80888

Description: The `iis-web.tpl: encoding` value from the `.config` file is overwritten by the Agent encoding value.

Platform: Independent

Subsystem: Application Configuration - Backend

Symptom: The encoding value specified in the `.config` file is overwritten by the Agent encoding value.

Resolution: Fixed.

QCCRID: 106203

Description: XML elements with single CDATA elements are not supported.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: The valueset editor is read only.

Resolution: Fixed.

QCCRID: 111027

Description: Application configuration and operating system support within a software policy is not consistent.

Platform: Independent

Subsystem: Application Configuration - Backend

Symptom: When loading an application configuration in a software policy, the application configuration must support all versions of all operating systems that the parent software policy supports. This does not apply to .zip files RPM's because they can support a single instance of RHEL, instead of every version the software policy supports. There is no parity between application configurations and virtually every other item in a software policy.

Resolution: Fixed.

QCCRID: 111558

Description: Unable to create localization files from folder.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: The Save operation cannot be completed because of missing data that is required.

Resolution: Fixed.

QCCRID: 111765

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

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: If you have "Read" or "None" privileges in OCCWeb ► Client Features ► Manage Installed Configuration and Backups on a server, SA will not be able to modify the application configuration value set for all scopes (Configuration, Facility, Customers).

Resolution: Fixed.

QCCRID: 111819

Description: Error message is incorrect after you set a previously scheduled job's date/time to a lapsed date/time.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: When you first create a scheduled job, you will get an error message if you enter a date that has already lapsed. When you edit the job by setting the date to one that has lapsed, you will get a different error message. You should get the same message because it is basically the same validation error.

Resolution: Fixed.

QCCRID: 111851

Description: Some servers fail during Configuration Compliance with an “integrity constraint” error.

Platform: Independent

Subsystem: Application Configuration - Backend

Symptom: When performing a compliance scan of application configurations and software policies for one or more servers, the scan can fail with error message “ORA-02292: integrity constraint (TRUTH.COMP_SUMM_COMP_DETAIL_FK) violated”.

Resolution: Fixed.

QCCRID: 111992

Description: The session_id in the compliance_summary table is null when running compliance for a software policy containing an application configuration.

Platform: Independent

Subsystem: Application Configuration - Backend

Symptom: Invalid data in the database (which is not visible in the user interface).

Resolution: Fixed.

QCCRID: 112119

Description: Provide the same name limitation for a renamed application configuration or template as that for a newly created one.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: The configuration table cell editor does not enforce character limitation and naming constraints.

Resolution: Fixed.

QCCRID: 112121

Description: Provide the same behavior for renamed templates with the blank name used for application configurations.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: The templates table cell editor does not enforce character limitation and naming constraints.

Resolution: Fixed.

QCCRID: 113689

Description: There is infinite loop behavior when previewing a file with a CML containing an unstable loop.

Platform: Independent

Subsystem: Application Configuration - CML Engine

Symptom: When parsing a unstable loop (a loop that has no target specified) the system would go in an infinite loop.

Resolution: Fixed.

QCCRID: 114041

Description: The Configured Applications tree does not get updated when attaching a software policy.

Platform: Windows 2008 R2 x64

Subsystem: Application Configuration - UI

Symptom: After upgrade to 9.01 but before the R2 Migration script is run, server AppConfig compliance status is correct (i.e. as they were before upgrade to 9.01). After R2 Migration script run, AppConfig compliance status of all migrated R2 servers are changed to Scan Needed.

Resolution: Fixed.

QCCRID: 114398

Description: "AppConfig", "Compliant", and "NonCompliant" compliance status is changed to "Scan Needed" after a Windows 2008 R2 migration.

Platform: Independent

Subsystem: Application Configuration - UI

Symptom: When attaching a software policy that contains an application configuration to a group, the Configured Applications tree is not updated.

Resolution: Fixed.

Application Deployment Manager

QCCRID: 104590

Description: Validate length of string fields before writing to avoid Oracle errors or multi-master restrictions

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If strings were too long, Oracle errors resulted.

Resolution: All fixed-length strings are now converted to UTF-8, and their length is checked before they are written to the database. Strings that are too long are truncated.

QCCRID: 107544

Description: Double-clicking in the Type column for a parameter results in an empty edited dialog that causes an error when you click OK.

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: In the Parameter Editor dialog, if you double-clicked in the Type column for a parameter, a useless dialog box opened. If you clicked OK in the useless dialog box, an error message appeared.

Resolution: If you double-click in the Type column, no dialog opens.

QCCRID: 109343

Description: Deleting a version leaves an empty version folder in SA Library

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you deleted a version in the Application Deployment Manager, an empty version folder remained in the SA Library.

Resolution: The version folder in the SA Library is now removed when you delete a version.

QCCRID: 110134

Description: Can initiate a deployment to a target with an empty tier (no servers in tier)

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: You could create and start a deployment job using a target that contained an empty tier. The Jobs log reported that the deployment job was successful, even though it did not do anything.

Resolution: The **Start** button on the Deployment screen is no longer available when a target contains an empty tier.

QCCRID: 110852

Description: No message is displayed if your Software Policy, Package, or Application Configuration search returns no items that match the tier platform

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you create or modify a Software Policy, Software Package, or Application Configuration component, you can search for pertinent library items and then select the one that you want to use. Previously, if your search returned no items that matched the platform of the tier, there would be no indication why the search results table was empty.

Resolution: If no search return items match the tier platform, a warning message to that effect is displayed.

QCCRID: 110875

Description: “Save Changes” dialog appears when there are no pending changes

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If you selected **Tools > HP Server Automation** when viewing the Administration screen in the Application Deployment Manager, the “Save Changes” dialog would appear regardless of whether changes were pending.

Resolution: The “Save Changes” dialog now appears only when changes are pending and you attempt to navigate away from the current context.

QCCRID: 111038

Description: Deployment screen shows settings from the previous session if no version is selected

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: On the Deployment screen, the following fields in the right panel should remain blank until you select a version and a target: Parameters, Changes, Comment, Rolling Deployment, and Scheduling. Previously, the settings used in a previous deployment editing session were not cleared.

Resolution: These fields are now cleared until you select a version and a target.

QCCRID: 111103, 111128

Description: Exception occurs when a long string is used to specify a parameter

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When adding or editing a parameter, if you entered more than 4000 characters in certain fields (Name, Value, Description, or Target Value), a cryptic error message would appear when you tried to save your changes.

Resolution: These fields are now truncated to the equivalent of 4,000 ASCII characters.

QCCRID: 111121

Description: Wrong special variables options appear in environment flow variables

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Server-specific special variables (such as Server Name or Server ID) and tier-specific special variables (such as Server names for Tier “Tomcat 6.0.20” or Server IDs for Tier “Tomcat 6.0.20”) should never appear in the list of available special variables used to define the values of parameters used by the Pre-Deployment and Post-Deployment flows for an environment. Previously, these special variables were available in this context.

Resolution: Fixed.

QCCRID: 111218

Description: Jobs screen items do not remain sorted correctly when an item is selected

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you selected an item on the Jobs screen, the items would be re-sorted, and the selected item would move somewhere else—possibly out of view.

Resolution: Fixed.

QCCRID: 111223

Description: Administration ► Environments page does not refresh after a failed operation

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If you attempt to create a new environment or modify an existing environment, and that operation fails, the Environments page does not refresh—which makes it appear that your operation was successful when, in fact, it was not.

Resolution: Fixed.

QCCRID: 111236

Description: Deleting non-empty tiers can cause a component of a deleted tier to replace a component of an existing tier

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: On the Applications screen, deleting a tier that contained one or more components corrupted other tiers.

Resolution: Fixed. Deleting one tier no longer affects other tiers.

QCCRID: 111325

Description: Tool-tip for Select Target drop-down menu is sometimes incorrect

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: On the Deployment screen, the tool-tip that appears when you mouse over the Select Target drop-down menu incorrectly displays the name of the last selected target when the label displayed is “No Targets” or “Select Target.”

Resolution: No tool-tip is displayed when the label is “No Targets” or “Select Target.”

QCCRID: 111398

Description: In the Manage Targets dialog, only one item is moved when multiple items are selected

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: The Manage Targets dialog enables you to select multiple targets and move them from one group to another. Previously, only one item was moved.

Resolution: All selected items are now moved.

QCCRID: 111500

Description: UI exception occurs when a user who does not have permission to Create Applications or Manage Application Deployment attempts to drill-down from the Jobs screen

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: See Description.

Resolution: If a non-superuser who does not have Create Applications or Manage Application Deployment for this SA core attempts to drill-down from the Jobs screen, an error message is now displayed. A superuser with View All Jobs permission is permitted to drill-down from the Jobs screen.

QCCRID: 111507

Description: “Server and policy platform mismatch” error occurs at deployment time when using tier policy

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If the server platform did not match the platform of the policy associated with the tier, a deployment job was started, but it immediately failed. This was inconvenient, since the mismatch should have been reported earlier.

Resolution: You are now warned that the job will fail because the platforms do not match. See [QCCRID: 110852](#) on page 44.

QCCRID: 111595

Description: Cancelling a job right after it start provides a confirmation message with no job ID

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If you cancelled a job that just started, the confirmation dialog contained a message that said: “Are you sure you want to cancel job?”.

Resolution: Confirmation message now reads, “Are you sure that you want to cancel the selected job?” if the job ID is not yet available.

QCCRID: 111656

Description: Backup or rollback fails for large for Code components

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Backup and rollback scripts for large Code components were failing, because the default timeout for these scripts was very short.

Resolution: You can now configure the timeout when you specify the Code component. The default setting is 3600 seconds (one hour). See “Code Components” under “Types of Components” in the *Application Deployment Manager User Guide*.

QCCRID: 111680

Description: The Windows Backup and Rollback scripts were not handling directory hierarchies correctly

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: For full releases, the Windows Backup script backed up files into multiple places and created too many files when the Source Directory had subdirectories. For delta releases, it did not back up files in subdirectories correctly.

Resolution: Fixed. Both the Backup and Rollback scripts now work correctly.

QCCRID: 111681

Description: Windows backup and rollback scripts don't work properly if drive letter is not specified for the Default Install Path

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: The deployment fails.

Resolution: Fixed. The ADM correctly resolves the path, adding the default drive letter to the beginning.

QCCRID: 111926

Description: Parameters grid on the Deployment screen should show components like the Component Editor does so that you can see where parameters come from

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: The Parameters grid on the Deployment screen did not show you which component was using each parameter.

Resolution: Fixed. The Parameters panel on the Deployment screen now contains a Component column.

QCCRID: 111959

Description: Multiple OO Flow components in an application cause parameters between them to be overwritten

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Parameter values were incorrect if an application included more than one OO Flow component.

Resolution: Fixed. Parameters now have correct values no matter how many OO Flow components are included.

QCCRID: 112013

Description: Parameter Editor shows wrong environment when selecting multiple targets

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If two or more environments contain targets with identical names, the incorrect environment is sometimes shown in the Parameter Editor dialog.

Resolution: The ADM now requires that all targets have unique names.

QCCRID: 112597

Description: Deployment fails without reporting why when the job is blocked pending approval

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Any SA job can be blocked pending approval. ADM deployment jobs are subject to this blocking. Previously, if an ADM deployment job failed because it was blocked pending approval, no message to that effect was displayed.

Resolution: Fixed. ADM now reports that the job is blocked and waits until it is either approved or disapproved (cancelled).

QCCRID: 112941

Description: "Name" special variables use SA names, not host names

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you used a special variable in a parameter to refer to a server, any output that contains the server name would show the SA name for that server, not the host name.

Resolution: Three new special variables were added: `server.hostname`, `deploy.servers.hostnames`, and `{tier["<name>"].server.hostnames}`. You can use these variables when you define parameter values.

QCCRID: 113127

Description: You can add deactivated servers to a target, but you cannot deploy to them

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Previously, you could add deactivated servers to a target. When you attempted to deploy, the deployment job would fail.

Resolution: Fixed. You can no longer add deactivated servers to a target.

QCCRID: 113283

Description: In the Select Targets dialog, an exception occurs when the Filter box is selected and there are no valid targets

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: The Filter box in the Select Targets dialog enables you to only show those servers whose platform matches the selected version. Previously, if you selected the Filter box, and there were no valid servers to choose from, you would see a cryptic error message.

Resolution: Fixed. If there are no valid servers, an empty tree is displayed.

QCCRID: 113342

Description: tar options used by the ADM are not valid on all platforms

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Deployment jobs for applications with Code components would fail on certain platforms.

Resolution: Fixed. Code components can now be successfully deployed on all supported platforms.

QCCRID: 113382

Description: Backup step on Solaris platforms incorrectly reports “nothing to back up”

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: During a deployment job to a Solaris target, the output of the backup step said that there were “No files to backup” when a backup was, in fact, performed.

Resolution: Fixed. The Backup script for UNIX code components was repaired.

QCCRID: 113426

Description: Code component changes list should be sorted

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: For a Code component with the Filesystem source type, the changes listed on the Deployment page when you select “Show Code Component Changes” should be sorted. Previously, it was not sorted.

Resolution: Fixed. The list is now sorted hierarchically (and alphabetically at each layer in the directory structure).

QCCRID: 113491

Description: Long Application Configuration names do not display correctly in the ADM

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If the name of an Application Configuration did not fit in the Name column in the Select Application Configuration dialog, a scroll bar was displayed. The scroll bar, however, covered up the name.

Resolution: The name is now truncated to fit in the column. You can see the complete name in the tool tip that appears when you mouse over the name in the table.

QCCRID: 113603

Description: Underscore character is not displayed in the Select Policy, Select Package, or Select OO Flow dialogs

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: In the Select Policy dialog, all underscore characters appeared to be missing in the policy Name column. This also happened in the Select Package and Select OO Flow dialogs. The problem was that the table rows were too short.

Resolution: Fixed.

QCCRID: 113785

Description: On the Permissions tabs in the Edit Application and Edit Environment dialogs, you should not be able to add the same user or group more than once

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Previously, you could add the same user or group to the list on the Permissions tab for applications and environments.


Resolution: Fixed. Users and groups that have already been added to the list are removed from the drop-down list of available choices.

QCCRID: 113283

Description: Name of “Revert” button is inconsistent

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: The function of the “Revert”  button is to discard any pending changes and reload the item from the database. The name is displayed in a tool-tip when you mouse over the button. The button had different names in different contexts, including Revert, Reset, Refresh, and Reload.

Resolution: Fixed. The name of this button is now “Revert [item]” in all contexts.

QCCRID: 113841

Description: No Distinction between Users and User Groups on Permission tabs

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: In the Edit Application and Edit Environment dialogs, there was no distinction between an individual user and a user group in the table on the Permissions tab.

Resolution: Fixed. There is now a Type column that says User or Group.

QCCRID: 113897

Description: Servers with “ESX” or “Unknown” OS should not be included in the Windows server selection list

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Previously, the Add Servers to Target dialog listed servers running ESX and servers in the “Unknown” OS category when you were adding servers to a Windows tier.

Resolution: Fixed. Only Windows OS servers are listed for Windows tiers; only UNIX servers are listed for UNIX tiers.

QCCRID: 113911, 114664, 114856


Description: When a job fails because the registry key is invalid, the job should complete with failure status

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If you specified an invalid registry key for a Windows Registry component, and you deployed the application, the deployment job would complete without error—even though the registry operation did not work. There was no indication anywhere that the registry change did not work.

Resolution: Fixed. All registry key names and values are now carefully validated when you save the component.

If the “Warning”  button appears on the Applications tool bar, this indicates that an invalid key name or value was detected. Click the button to learn how to fix it. If you do not fix the errors prior to deployment, this button will also appear on the Deployment screen. You will not be able to deploy the application until you fix the errors.

QCCRID: 113965, 115706

Description: Deploying a Code component with the Filesystem source type does not preserve symlinks on target

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If there are symbolic links (symlinks) in the source directory for your Code component, those symlinks were not preserved or recreated on the targets.

Resolution: Fixed.

QCCRID: 114197

Description: Searching for an OO Flow with no characters in the Search box fails

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Previously, if you clicked the Search button in the Select OO Flow dialog, and you had not entered anything in the text box, the search would time out without returning any items.

Resolution: Fixed. This search matches full words in the OO Flow name. If you do not enter anything in the “Full word” box, you are now warned that searching without supplying a full word could take minutes. The timeout was also increased to 18 minutes. If no items are found that contain your search word, you now get a message to that effect.

QCCRID: 114666

Description: Binary registry key value is displayed as hex

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: In the Add Value dialog, when you selected Binary as the value type, the value would be displayed in hexadecimal.

Resolution: Fixed. Displayed in binary now.

QCCRID: 114764

Description: Prevent users from rolling back or undeploying earlier versions

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Previously, if you initiated roll back or undeploy of a version that was older than the most recently deployed version of the same application, you were not warned about or prevented from doing that. This is dangerous and strongly discouraged.

Resolution: Now, you are warned if you attempt to roll back or undeploy an older version. You must confirm your intention to proceed.

QCCRID: 114918

Description: DWORD value entered in decimal not created

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: In a Windows Registry component, if you specified the value of a DWORD type key using decimal characters, the key would not be created. Only hexadecimal characters worked.

Resolution: Fixed. Decimal values are now converted to hexadecimal. DWORD type keys are now validated when you save the component.

QCCRID: 114921

Description: Jobs appear to be (perpetually) in progress when ADM is restarted

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: If the ADM is stopped, any deployment jobs that were running at the time never complete and appear to be IN_PROGRESS in perpetuity.

Resolution: Fixed. If the ADM stops and restarts, any deployment jobs that were in progress are examined to determine what action needs to be taken. If a job step was in progress when the ADM stopped, the job is marked FAILED and rollback is initiated. If all job steps were successfully completed, the job can be marked Completed.

QCCRID: 115117

Description: Need horizontal scrollbar in “Add Servers to Target” dialog

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you opened a hierarchy of Device Groups—such as Public : Opsware : Operating System : All Linux : All Linux Red Hat—you could not see the full names of the child device groups, because they were truncated and there is no horizontal scroll bar.

Resolution: Fixed. Scroll bar added.

QCCRID: 115184

Description: Server count resets to 1 in Rolling Deployment settings update

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you attempted to change the server count for a Rolling Deployment, the value was always reset to one (1) after you saved your changes.

Resolution: Fixed. The value you enter is now saved and honored.

QCCRID: 115204

Description: “Failure parsing template” error reported after an Application Configuration is selected

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you selected an Application Configuration, if the Application Deployment Manager failed to parse the template used with the Application Configuration, and cryptic error messages were reported.

Resolution: Fixed. The ADM now parses properly formed Application Configuration templates correctly. If a failure occurs, a more meaningful error message is displayed.

QCCRID: 115209

Description: Should not be able to select the same Package more than once

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When you were creating a Package component, you could add the same Package more than once. This did not make sense.

Resolution: Fixed. You can only select a Package once.

QCCRID: 115367

Description: Incorrect Job ID referenced in confirmation message for rollback or undeploy

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When trying to roll back or undeploy a version with OO Flow or Configuration File components, the following confirmation message is displayed:

Are you sure you want to rollback job '0'?

Are you sure you want to undeploy job '0'?

Resolution: Fixed. Message either uses the real Job ID or references “the selected job” instead.

QCCRID: 115368

Description: Rescheduled cut over time not in-sync

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Say that you scheduled a deployment job to stage immediately but cut over at a different time. Later, you changed your mind and modified the scheduled cut over time to be on a different date.

The time displayed in the “Wait for Cut Over Time” job step was different than the time displayed in the Reschedule Job dialog, and this was confusing.

Resolution: The text in the cutover job step Output box is static, so it will not change when you reschedule a job. To reduce confusion, this text now reads, “Job will resume at scheduled Cut Over Time.” The originally scheduled cut over time is shown in the Step Details dialog.

QCCRID: 115534

Description: Deleted release name is not reusable

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: Previously, if you deleted a release, you could not ever use its name again.

Resolution: Fixed. You can now recycle release names.

QCCRID: 115546

Description: ADM experiences memory problems when there are many Code component changes to show

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: When creating a new version of a full release, if you selected “Show Code Component Changes,” and there was a very large number of files included in the Code components, you might see cryptic “out of memory” error messages.

Resolution: The number of files in a Code component is now limited to 100,000 for a full release.

QCCRID: 115949

Description: The Parameter Values dialog is not rendering correctly

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: In the Parameter Editor, if you double-clicked a parameter value, the Parameter Values dialog opened, but it did not render correctly.

Resolution: Fixed. The Value field is now limited to 300 characters, and you can use the arrow keys to display additional character.

Audit and Remediation

QCCRID: 81358

Description: There is "hex_ntop failed" data for a snapshot on IIS Metabase object.

Platform: Windows

Subsystem: Audit and Remediation - Backend

Symptom: If the data type of the metabase entry is binary and there is no actual data, the snapshot shows "hex_ntop failed" as the data.

Resolution: Fixed.

QCCRID: 105021

Description: The Audit Results browser contains miscellaneous, invalid characters (such as " : 0 ") that should be removed.

Platform: Independent

Subsystem: Audit and Remediation - UI

Symptom: Miscellaneous, invalid characters, such as " : 0 ", display in the Audit Results browser.

Resolution: Fixed.

QCCRID: 105146

Description: In the Audit Policy window, in the Properties Name, the text field should be enabled and prompt for input when you select New to create an audit policy.

Platform: Independent

Subsystem: Audit and Remediation - UI

Symptom: In the Audit Policy window, the Properties Name, the text field is not enabled and you are not prompted for input to create a new audit policy.

Resolution: Fixed.

QCCRID: 108616

Description: When you rename an instance of compliance check, the new name displays in the lower pane, while the old (previous) name displays in the top pane.

Platform: Independent

Subsystem: Audit and Remediation - UI

Symptom: When you rename an instance of compliance check, the new name does not display in the details pane.

Resolution: Fixed.

QCCRID: 110611

Description: A snapshot with the perform inventory option shows no warning to upgrade the Agent when selecting items that are not supported by an old Agent version (SMOs).

Platform: Independent

Subsystem: Audit and Remediation - Server Module

Symptom: A snapshot with the perform inventory option should show a warning that SMO rules selected for an audit cannot be run.

Resolution: Fixed.

QCCRID: 110811

Description: The compare .config file audit did not detect differences when comparing link files.

Platform: Unix

Subsystem: Audit and Remediation - Backend

Symptom: The file selected for file configuration comparison is a symbolic link and the audit does not show the correct results. Audit runs the file as a regular file system rule.

Resolution: Fixed.

QCCRID: 111682

Description: The View button and Contents panel do not display for the "Application Configurations" rule in the Snapshot Specification window. No application configuration rule can be added for the snapshot.

Platform: Independent

Subsystem: Audit and Remediation - UI

Symptom: When the View button and Contents panel does not display for the "Application Configurations" rule in the Snapshot Specification window, no application configuration rule can be added for the snapshot.

However, you can save and run the snapshot. If you specify the snapshot as the Source for a later audit, the following error message displays: "The policy provided has no rules in it". This is because the snapshot has no rule selected.

Resolution: Fixed.

QCCRID: 111791

Description: The stempcache directory is not automatically cleaned up when there is an audit failure.

Platform: Independent

Subsystem: Audit and Remediation - Backend

Symptom: If an audit fails in the middle of execution, temporary files created in compliancache/stempcache are not cleaned up and the directory continues to grow.

Resolution: Fixed.

QCCRID: 113305

Description: Move Compliance view in Management Policies panel.

Platform: Independent

Subsystem: Audit and Remediation - UI

Symptom: The ordering of the menu items in the Management Policies panel should be changed.

Resolution: Fixed.

QCCRID: 116286

Description: Checks in audit policies provided from HPLN do not use the displayName rule.

Platform: Independent

Subsystem: Audit and Remediation - UI

Symptom: When renaming and saving an instance of a compliance check in the Audit Policy or Audit Task browser, the new name does not display when you reopen the browser.

Resolution: Fixed.

QCCRID: 116514

Description: Dataminer will not mine CIS 1.5 audit results.

Platform: Independent

Subsystem: Audit and Remediation - Backend

Symptom: There is a pluggable check in the audit policy whose operator is mapped to the "Does not match Regular Expression (ignore case)" string. This string happens to be larger than the operator column in the COMPLIANCE_DETAIL table. This causes an Oracle error and aborts the transaction. Data is not written to the Model Repository and, subsequently, no data can be mined for the reports.

Resolution: Fixed.

Extensible Discovery

QCCRID: 110987

Description: The get_firmware.sh script does not apply to SuSE 10 SP3 PPC64.

Platform: SLES10 SP3 PPC64

Subsystem: Extensible Discovery

Symptom: The Extensible Discovery get_firmware.sh script does not support the PPC64 platform.

Resolution: Fixed.

Global File System

QCCRID: 110903

Description: Server browser shows error "500 OGFS view dir does not exist SA".

Platform: Windows managed server with locale set to S-Chinese (Code Page CP936)

Subsystem: Global Filesystem - Shell Backend

Symptom: Unable to access the file system of managed servers via OGFS.

Resolution: Fixed.

QCCRID: 112418

Description: Solaris panic BAD TRAP: type=31 rp=2a103a81400 addr=0 mmu_fsr=0 occurred in module "unix" due to a NULL pointer.

Platform: Solaris 5.10

Subsystem: Global Filesystem - Shell Backend

Symptom: There is a Solaris kernel panic.

Resolution: Fixed.

QCCRID: 112419

Description: panic Deadlock: cycle in blocking chain.

Platform: Solaris 5.10

Subsystem: Global Filesystem - Shell Backend

Symptom: There is a Solaris kernel panic.

Resolution: Fixed.

Installer

QCCRID: 76655

Description: Make `get_slice_ips.py` more user friendly.

Platform: Linux/3AS, Linux/4AS, Linux/5Server, SunOS

Subsystem: Installer

Symptom: /opt/opsware/oi_util/bin/get_slice_ips.py was designed as a tool to be used internally by the Installer and, as such, was not prepared for the types of errors a user might introduce. When problems occurred, it responded with vague errors that were not helpful.

Resolution: Fixed.

ISM Tool

QCCRID: 110511

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

Platform: Windows Server 2008 (x86)

Subsystem: ISM Tool

Symptom: The ismtool does not correctly recognize a Windows Server 2008 (x86) server.

Resolution: Fixed.

QCCRID: 111304

Description: ISMtool is not supported on Windows Server 2008 R2 servers in 7.5.x 7.8.x and 9.0.

Platform: Windows Server 2008 R2 x64

Subsystem: ISM Tool

Symptom: Information about the created ISM shows supported platform as 'Windows 2000' instead of "Windows Server 2008 R2 x64".

Resolution: Fixed.

QCCRID: 111662

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

Platform: Windows 2003 x64, Windows 2008 x64, Windows Server 2008 R2 x64

Subsystem: ISM Tool

Symptom: The control job fails for ISMs built using the ZIP package engine on Windows 64-bit servers.

Resolution: Fixed.

Jobs and Sessions

QCCRID: 111800

Description: The server count is shown as zero (“0”) when there is one server present in an Application Deployment job.

Platform: Independent

Subsystem: Jobs & Sessions

Symptom: Jobs in the job logs display show “0” servers in the Server column.

Resolution: Fixed.

QCCRID: 111802

Description: Application Deployment Manager (ADM) job groups sometimes stop refreshing in the user interface. The refresh rate is also too slow.

Platform: Independent

Subsystem: Jobs & Sessions

Symptom: Live ADM jobs fail to update their real-time state in the Job Dialog window.

Resolution: Fixed.

QCCRID: 111856

Description: The Application Deployment Manager (ADM) Job Group display is incorrect for Run Program Extension.

Platform: Independent

Subsystem: Jobs & Sessions

Symptom: Copy_configs job always runs from the core server. This was not displayed.

Resolution: Fixed.

Model Repository

QCCRID: 83813

Description: Unable to sync differences in ServiceInstances after a referenced device has been deleted.

Platform: Independent

Subsystem: Model Repository

Symptom: Attempts to synchronize a multimaster difference on a ServiceInstance fail with an error similar to:

```
ERROR -- Unable to perform UPDATE!
spin.genericDatabase error: 'ORA-02291: integrity constraint (.) violated -
parent key not found
ORA-06512: at "TRUTH.SERVICE_INSTANCES_DVC_ID_RTRG", line 14
ORA-01403: no data found
ORA-04088: error during execution of trigger
'TRUTH.SERVICE_INSTANCES_DVC_ID_RTRG' during 'UPDATE service_instances SET
mod_dt = TO_DATE(:p1, 'DD-MON-YYYY HH24:MI:SS'), tran_id = :p2 WHERE
(srvc_inst_id = :p3)' with args ('20-OCT-2008 23:40:21', '124970002',
'3230002')
```

Resolution: Fixed.

QCCRID: 93757

Description: Database user TRUTH statistics collection job fails with error: ORA-01000: maximum open cursors exceeded.

Platform: Independent

Subsystem: Model Repository/Oracle RDBMS 11.1.0.7

Symptom: This error is intermittent and not all customers will run into this issue. The error is caused due to an Oracle bug (#7651092).

You will see the errors in Oracle's alert.log file. The errors are similar to the following:

```
<timestamp>
Errors in file /u01/app/oracle/diag/rdbms/truth/truth/trace/
truth_j001_4653.trc:
ORA-12012: error on auto execute of job 1
ORA-01000: maximum open cursors exceeded
ORA-06512: at "SYS.DBMS_STATS", line 18566
ORA-06512: at "SYS.DBMS_STATS", line 19051
ORA-06512: at "SYS.DBMS_STATS", line 19132
ORA-06512: at "SYS.DBMS_STATS", line 19088
ORA-06512: at line
```

Resolution: Fixed

Before running the patch install script, perform steps shown in [Database Schema Update Procedure](#) on page 27 to ensure that the script 20_truth_modify_truth_stats_job_90.sh script is run during patch installation.

OS Provisioning

QCCRID: 65480

Description: Import Media script should support long filenames for SMB.

Platform: Independent

Subsystem: OS Provisioning - Backend

Symptom: It is difficult to translate long filenames to 8.3 syntax format when there is no unique naming capability in the directory structures. It takes a long time to translate these paths into the 8.3 syntax.

Resolution: Fixed.

QCCRID: 89108

Description: An error in the OS Provisioning job is not shown in the Job Status Error tab.

Platform: ESX, Linux, Solaris, VMware, Windows, Windows 2000, Windows 2003, Windows 2008, Windows XP

Subsystem: OS Provisioning - Backend

Symptom: If OS provisioning fails, the OS provisioning Job Status window does not show the cause of the error in the Job Status Error tab.

Resolution: Fixed.

QCCRID: 93881

Description: You can upload an `unattend.xml` file that exceeds the maximum size allowed.

Platform: Windows 2008

Subsystem: OS Provisioning - OCC - Web

Symptom: An error occurs when using Prepare OS for a Windows 2008 OS Profile that has an `unattend.xml` file that exceeds the 256K default size value. During the Prepare OS process, this `.xml` file is allowed to upload; however, subsequently, an error occurs when you try to access the Installation tab.

Resolution: Fixed.

To change the maximum size of the `unattend.xml` file, completed the following steps:

- 1 Add the following parameter to the `/etc/opt/opsware/twist/twistOverrides.conf` file:

```
customattr.maxsize=XXXXXX
```

XXXXXX is the desired size in bytes.
- 2 Restart the Web Services Data Access Engine (twist).

QCCRID: 95401

Description: The autoprovision for `registerManagedNodeForDS` would always send kickstart information through `eth0`.

Platform: Linux

Subsystem: OS Provisioning - Backend

Symptom: If the server being provisioned has multiple network cards, SA may not consistently use one card throughout provisioning, which may cause provisioning failures.

Resolution: Fixed.

QCCRID: 109925

Description: winpe-ogfs booted servers were listed in the Data Integrity Error fail test.

Platform: Windows

Subsystem: OS Provisioning

Symptom: When running the System Diagnostics, invalid errors are shown in the Data Integrity section.

Resolution:

QCCRID: 111245

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

Platform: Linux

Subsystem: OS Provisioning

Symptom: If you locally change (overwrite) the value of this system configuration parameter in the SA installation, the upgrade process will preserve the value. This is often the correct behavior, but in this specific case the correct behavior would be to overwrite the data with the new data shipped with the SA product.

Resolution: Fixed.

QCCRID: 111445

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

Platform: Independent

Subsystem: OS Provisioning - Backend

Symptom: When OS sequences are run, device group privileges for the user running the job should be escalated; however, they are not, resulting in provisioning failures.

Resolution: Fixed.

QCCRID: 111845

Description: The `sequence_id` and MAC link were not removed for Solaris10x86 provisioning that was done using MBC.

Platform: Linux

Subsystem: OS Provisioning - MBC

Symptom: Solaris servers provisioned using MBC would continually reboot into the pxe provisioning menu.

Resolution: Fixed.

QCCRID: 113004

Description: Remediate job using OS Build Plans failed intermittently in cross mesh test.

Platform: Windows 2003

Subsystem: OS Provisioning - Backend

Symptom: Remediate jobs launched from OS Build Plans may fail with an error.

Resolution: Fixed.

QCCRID: 113056

Description: import_media does not correctly detect the .wim image URL.

Platform: Windows

Subsystem: OS Provisioning

Symptom: If there is a path to a provided directory (not to a .wim file), import media will succeed, instead of producing an error that prompts you to specify the path to a file. If a directory is specified, the provisioning will fail. Even if there is a .wim image, the provisioning will fail because the mrl does not end in .wim and parseunc(mrl) will set the image as None, causing the build scripts to run setup.exe (which does not exist), instead of imagex.exe.

Resolution: Fixed.

QCCRID: 114303

Description: The monitorServerBuildInit is never executed for OEL and CentOS.

Platform: OEL 4, OEL 5, CentOS 5

Subsystem: OS Provisioning

Symptom: When provisioning a server with OEL 4, 5 and CentOS 5 after rebooting to the OS installer, the following warning displays: "Buildscript cannot verify that the second stage installer matches the requested OS version."

Resolution: Fixed.

QCCRID: 114403

Description: Solaris 10 U8 mini-root shipped with 7.80.03 causes kernel panic during provisioning of Solaris 10 U6 servers with ZFS.

Platform: Solaris

Subsystem: OS Provisioning

Symptom: When provisioning Solaris 10 U6 from the mini-root provided with 7.80.03 (Solaris 10 U8), the newly provisioned machine will kernel panic when trying to mount the ZFS disk due to a version discrepancy.

Resolution: Fixed.

QCCRID: 103377

Description: The following a prepdisk error occurs on some Linux installs: "prepdisk.py failed: Incomplete arguments".

Platform: Linux

Subsystem: OS Provisioning - Backend

Symptom: A provisioning job fails with an error, such as "java.lang.NoSuchMethodError".

Resolution: Fixed.

QCCRID: 107141

Description: Run action is enabled in the OS Build Plan window for a user who does not have the "Allow Execute OS Build Plan" privilege.

Platform: Independent

Subsystem: OS Provisioning

Symptom: You can select Action ► Run when you do not have the required privileges.

Resolution: Fixed.

QCCRID: 110077

Description: Removing steps from the OS Build Plan causes a Null Pointer Exception (NPE).

Platform: Windows 2003, Windows 2008

Subsystem: OS Provisioning - UI

Symptom: An NPE is found in logs when you remove a step from the OS Build Plan.

Resolution: Fixed.

Patch Management

QCCRID: 92124

Description: The Manage Windows Patch Policy READ privilege allows you to change the availability of Windows and Solaris patches.

Platform: Solaris, Windows

Subsystem: Patch Management - Windows and Patch Management - Solaris

Symptom: The user interface appeared to allow users with inadequate privileges to change the availability setting of patches.

Resolution: Fixed.

Patch Management for Solaris

QCCRID: 110313

Description: In Advanced Search, there is a misspelled word in the Patch "Where" drop-down list.

Platform: Sun OS 5.01, 5.10 x86, 5.9, 5.8, 5.7, 5.6

Subsystem: Patch Management - Solaris

Symptom: In Advanced Search, there is a spelling error in the "Where" drop-down list. "Reboot Immediae on UnInstall" should read "Reboot Immediate on UnInstall".

Resolution: Fixed.

QCCRID: 112588

Description: The Add to Patch Policy option should be enabled when a Solaris patch or patch cluster is selected from Library ► By Type ► Patches ► Solaris ► SunOS 5.x.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: Cannot attach a patch or patch cluster to a patch policy when you select Library ► By Type ► Patches ► Solaris ► SunOS 5.x.

Resolution: Fixed.

QCCRID: 113591

Description: The solpatch_import filter option excludes obsoleted, recommended patches.

Platform: Sun OS 5.01, 5.10 x86, 5.9, 5.8, 5.7, 5.6

Subsystem: Patch Management - Solaris

Symptom: On June 4, 2010, Oracle changed the process of tagging patches as "recommended". After June 4, 2010, only the first patch to fix a Sun Alert issue is tagged "recommended". Before June 4, 2010, the behavior was that the latest patch to include the fix would be tagged "recommended" and the "recommended" tag would be removed from the obsoleted patch.

Resolution: Fixed.

Patch Management for Unix

QCCRID: 110273

Description: Patch installation fails for AIX 5.3 for EMR3 Agent 32h.0.0.101 without a specific error message; After the Agent is upgraded, the patch installation is successful.

Platform: AIX

Subsystem: Patch Management - Unix - Backend

Symptom: When you try to install a patch on an AIX 5.3 server that has the EMR3 Agent on it (version 32h.0.0.101), the installation fails and no specific error message is displayed.

Resolution: Fixed.

Patch Management for Windows

QCCRID: 111964

Description: Incorrect tooltip for patch compliance when the patch is in the list of installed patches, has the "Never Install" exception set, and is not in a patch policy.

Platform: Windows

Subsystem: Patch Management - Windows

Symptom: When an installed patch is not in a patch policy, setting the "Never Install" exception on it from the list of installed patches, the tooltip says: "Installed but policy and exception say not to".

Resolution: Fixed.

QCCRID: 110340

Description: Remediate shows a "Will Not Install" status for "Always Install" exceptions for a different platform than the managed server when the "Always Install" exception is at the server group level.

Platform: Any platform that is not the same as the managed server

Subsystem: Patch Management - Windows

Symptom: A "Will Not Install" status (for a patch) during remediation displays when a server group has an "Always Install" exception whose platform does not match the managed server.

Resolution: Fixed.

QCCRID: 110391

Description: Windows Server 2008 R2 patches are displayed in the patch library as Windows Server 2008 (x86) patches.

Platform: Windows 2008

Subsystem: Patch Management - Windows - Backend

Symptom: The patch library is showing Windows Server 2008 R2 patches in the Windows Server 2008 (x86) patch library.

Resolution: Fixed.

QCCRID: 111862

Description: Remediate of managed server with a group "Never" exception and a device "Always" exception causes a non-install due to the "Never" exception.

Platform: Windows

Subsystem: Patch Management - Windows

Symptom: The group "Never" exception overwrites the device "Always" exception.

Resolution: Fixed.

QCCRID: 114337

Description: Windows patches that have more than 6 digits in their KB numbers do not have correct unit_name and unit_display_name values in the recommended_patches and installed_units tables.

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: SA needs to support 7 digit KB numbers.

Resolution: Fixed.

SA Client

QCCRID: 81123

Description: There are other HP rebranding items for a future release.

Platform: Independent

Subsystem: SA Client - Framework

Symptom: There are several rebranding items for a future release.

Resolution: Fixed.

QCCRID: 91685

Description: A new, saved search does not display in the drop-down selection list.

Platform: Independent

Subsystem: SA Client - Search

Symptom: Updates on a saved search combination model (such as create and delete) are not reflected in the user interface.

Resolution: Fixed.

SA-OO Integration

QCCRID: 111738

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

Platform: Independent

Subsystem: SA-OO Integration

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

Resolution: Fixed.

QCCRID: 111740

Description: Ticket_ID is automatically filled for Run Flow Job.

Platform: Independent

Subsystem: SA-OO Integration

Symptom: When you did not provide any value for Ticket ID for Run Flow Job, a default value was automatically filled.

Resolution: Fixed.

QCCRID: 112466

Description: Flow integrations informational text says "Job Approvals", instead of "Job Blocking".

Platform: Independent

Subsystem: SA-OO Integration

Symptom: When you select Administration ► Flow Integrations, the descriptions on the right panel show "Job Approvals". This should say "Job Blocking".

Resolution: Fixed.

SAS Web Client

QCCRID: 111394

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

Platform: Independent

Subsystem: SAS Web Client

Symptom: If the existing user group has OGFS privileges for multiple users/logins, not all OGFS privileges for multiple users are copied to a cloned user group. For example, if a user group that is going to be cloned has OGFS privileges, the user group clone will work only if the privileges are for one user/login. If there are multiple users/logins for a privilege, only one user/login privilege is copied into the new cloned group and the rest of the users/login privileges are ignored.

Resolution: Fixed.

QCCRID: 114769

Description: Allow the ability to grant Global File System privileges in the SAS Web interface when the username contains a dash (-).

Platform: Independent

Subsystem: OCC Web - Administration

Symptom: Customer wants to use a username that contains a dash (-).

Resolution: Fixed.

Server Automation Visualizer

QCCRID: 94138

Description: Found "Error Running SiteMap" in the user interface for an HPUX11iv3 with multiple SAN devices and switches connected.

Platform: HPUX 11.31

Subsystem: Server Automation Visualizer - SiteMap

Symptom: Displaying sitemap causes an error and fails to display data.

Resolution: Fixed.

QCCRID: 110100

Description: A question mark (?) icon displays for Cent OS after a scan.

Platform: CentOS

Subsystem: Server Automation Visualizer

Symptom: There is a question mark (?) icon instead of the Cent OS icon in the user interface after a scan.

Resolution: Fixed.

Server Module

QCCRID: 88807

Description: IIS - Inventory fails on Italian/German/Korean/Japanese managed server using IIS SM.

Platform: Windows Server 2008

Subsystem: Server Module - IIS7

Symptom: IIS 7 SMO is failing because the `xml.dom.minidom.parseString` could not handle the output returned after executing the `appcmd` command in DOS for retrieving the values.

Resolution: Fixed.

QCCRID: 91597

Description: When run on VMware ESXi servers, server modules give a false and, potentially, alarming error message.

Platform: VMware ESXi

Subsystem: Server Module - Backend

Symptom: Server modules gives a false and potentially alarming error message.

Resolution: Fixed.

QCCRID: 107867

Description: Site and Application features are not remediated in IIS7 SM.

Platform: Windows Server 2008

Subsystem: Server Module - IIS7

Symptom: The remediation of features from "Site" and "Application" Level is not implemented in IIS 7 SMO. Only the features from the "Web Server Level" supports remediation.

Resolution: Fixed.

QCCRID: 111503

Description: Remediation of Test sites does not copy all values from the source to the target.

Platform: Windows Server 2008

Subsystem: Server Module - IIS7

Symptom: Machine Key and Providers features are implemented in IIS7 SMO only for the "Web Server Level". The "Site Level" does not support these features.

Resolution: Fixed.

QCCRID: 111521

Description: SMO_Users and Groups - Failed to add a user to the target on Windows 2000 during a remediate operation.

Platform: Windows 2000

Subsystem: Server Module - Users and Groups

Symptom: When a user from a managed server with a newer version of Windows 2000 is remediated on a Windows 2000 server, the Server Module produces an error.

Resolution: Fixed.

QCCRID: 112489

Description: Environment verbs should not be evaluated.

Platform: Windows Server 2008

Subsystem: Server Module - IIS7

Symptom: Some parts of the IIS7 server module evaluate %WINDIR% as C:\Windows when auditing various settings (and/or content), causing mismatches when performing audits.

Resolution: Fixed.

QCCRID: 112529

Description: IIS7 Server Module audit and remediation issue with several applications in the application pool.

Platform: Windows Server 2008

Subsystem: Server Module - IIS7

Symptom: The "Number of Applications" contained in an "Application Pool" is a read-only column and should not be included in remediation for an Application Pool.

Resolution: Fixed.

QCCRID: 113052

Description: Remediation of an error page without subStatusCode creates an error page with subStatusCode=0 on the target.

Platform: Windows Server 2008

Subsystem: Server Module - IIS7

Symptom: IIS7 SMO should add subStatusCode only if there is a subStatusCode attribute on the error page from the Source Server.

Resolution: Fixed.

QCCRID: 113804

Description: Failed to create providers on Web Server Level.

Platform: Windows 2008

Subsystem: Server Module - IIS7

Symptom: There is no distinction between remediation of providers feature from Web Server-Level and remediation of providers from Site-Application Level. The first uses the root path for setting providers, while the second uses the path of the Site or Application.

Resolution: Fixed.

Software Management

QCCRID: 112589

Description: Cannot add a Solaris patch to a patch policy from the patch's Patch Policies view.

Platform: Solaris

Subsystem: Software Management - UI - Software Policy

Symptom: There is a missing feature to add a Solaris patch to a patch policy from the Patch Policy view

Resolution: Fixed.

QCCRID: 112702

Description: The popup menus for a folder in the folder tree are enabled differently, compared to the folder list.

Platform: Independent

Subsystem: Software Management - UI - Library

Symptom: Popup menus are enabled differently for a folder in the folder tree compared to the folder list.

Resolution: Fixed.

QCCRID: 114781

Description: A Null Pointer Exception (NPE) occurs when you try to remediate a detached policy.

Platform: Independent

Subsystem: Software Management - API - Software Policy

Symptom: An error occurs when attempting to perform a remediation of a simultaneous attachment and detachment.

Resolution: Fixed.

QCCRID: 111793

Description: When there are Remediate job option settings changed after previewing, you cannot preview again.

Platform: Independent

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

Symptom: Changing options in the Remediate job window and previewing more than once fails.

Resolution: Fixed.

QCCRID: 111861

Description: After you add or delete policy items in a software policy and then save them, you are subsequently unable to open the software policy. There are Null Pointer Exceptions (NPEs) in the Java console. You must log off and then log back in to the SA Client.

Platform: Independent

Subsystem: Software Management - UI - Software Policy

Symptom: Adding and deleting items to a software policy while it is running in the remediate mode may prevent you from being able to re-open it.

Resolution: Fixed.

SE Connector

QCCRID 93313

Description: When you are creating a new access control, if you type the SE user name in the wrong case (SE is case sensitive about usernames) and then try to edit the SE Scanner access control to change the case (such as from lowercase to uppercase or vice versa), the changes are not implemented in the access control. This occurs when the user name contains all of the same letters and numbers as the user name that was originally entered, but only the case of the letters has changed.

Platform: Independent

Subsystem: SE Connector

Symptom: Editing SE Scanner access controls to change the case of letters in the username (from uppercase to lowercase or from lowercase to uppercase) does not work. This occurs when the name contains all of the same letters and numbers as the originally entered name, but only the case of the letters has changed.

Resolution: Edit the access control and completely change the username. Apply these changes. Edit the access control again and then change the username to the correct name in the correct case. Apply these changes.

QCCRID 93316

Description: When you are creating a new access control, if you type the password in the wrong case (SE is case sensitive about passwords) and then try to edit the SE Scanner access control to change the case (such as from lowercase to uppercase or vice versa), the changes are not implemented in the access control. This occurs when the password contains all the same letters and numbers as the password that was originally entered, but only the case of the letters has changed.

Platform: Independent

Subsystem: SE Connector

Symptom: Editing SE Scanner access controls to change the case of letters in the password (from uppercase to lowercase or from lowercase to uppercase) does not work. This occurs when the password contains all of the same letters and numbers as the password that was originally entered, but only the case of the letters has changed.

Resolution: Fixed. Edit the access control and completely change the password. Apply these changes. Edit the access control again and then change the password to the correct password in the correct case. Apply these changes.

Storage Host Agent Extension

QCCRID 100922

Description: When an HP-UX 11.23 server is presented with a LUN via dual port HBA, the user interface shows only one FC target mapping.

Platform: HP-UX 11.23

Subsystem: Storage Host Agent Extension

Symptom: The NGUI panel Inventory->Storage->Volumes->[Select Access Path View]->Select a LUN presented via dual ports HBA, the bottom panel will show only one target mapping instead of two entries. This occurs when an HBA driver does not support the SNIA HBA 2.0 version.

Resolution: Fixed.

QCCRID 101464

Description: For LUNs managed by Solaris Native MPXIO, the multipath count is displayed as 1. This behavior is seen on Solaris versions before Solaris 5.10 Update 3.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: For Solaris versions before Solaris 5.10 Update 3, the Storage Host Agent Extension inventory snapshot specification fails to discover the information related to Solaris Native MPXIO software. Because of this, MPXIO managed multipathed LUNs will have their path count as 1.

Resolution: Fixed.

Virtual Center

QCCR1D: 109849

Description: You receive an Exception error when you try to manage a Virtual Center (VC) if that VC has an SA-managed hypervisor.

Platform: ESX

Subsystem: Virtual Center

Symptom: Virtual Center (VC) exception error.

Resolution: Fixed.

QCCR1D: 109887

Description: Snapshot views of hypervisors that are managed by Virtual Center (VC) are not supported.

Platform: ESX, ESXi

Subsystem: Virtual Center

Symptom: Cannot see snapshot views.

Resolution: Fixed. Support for these snapshots has been added.

QCCR1D: 111780

Description: Hypervisors are not loading.

Platform: ESX

Subsystem: Virtual Center

Symptom: Hypervisors are not loading.

Resolution: Fixed.

QCCR1D: 115353

Description: Storage Panel page of the Storage Snapshot is not displayed when a hypervisor is managed through Virtual Center (VC) in the SA Client.

Platform: ESX, ESXi

Subsystem: Virtual Center

Symptom: Storage Panel page of the Storage Snapshot is not displayed.

Resolution: Fixed.

QCCR1D: 113887

Description: Create Virtual Machine job fails to boot the virtual machine into the server pool.

Platform: ESX, ESXi

Subsystem: Virtual Center

Symptom: Create Virtual Machine job fails to boot the virtual machine into the server pool.

Resolution: Fixed.

QCCR1D: 113891

Description: Cannot create *and* provision an ESX virtual machine guest.

Platform: ESX, ESXi

Subsystem: Virtual Center

Symptom: Cannot create *and* provision an ESX virtual machine guest.

Resolution: Fixed.

Virtualization

QCCR1D: 71640

Description: When an imported LDAP user clicks the Next button in the Create Virtual Zone wizard's Zone Definition step, they do not advance to the next step. The following NullPointerException error is returned:

```
WARNING init(NguiUser:-1): No user date format specified, using JVM defaults
java.lang.NullPointerException
at com.opsware.ngui.virtual.task.ZoneDataSpecificationPanel$
ServerVirtualizationZonePanel.createPanel(Unknown Source)
.....
at java.awt.LightweightDispatcher.dispatchEvent(Container.java:3128)
at java.awt.Container.dispatchEventImpl(Container.java:1613)
```

Platform: Windows

Subsystem: Virtualization

Symptom: A NullPointerException is received when users click the Next button in the Create Virtual Zone wizard.

Resolution: Fixed.

QCCRID: 71995

Description: The progress bar does not stop.

Platform: Independent

Subsystem: Virtualization - UI

Symptom: The progress bar does stop after opening a Virtualization object browser.

Resolution: Fixed.

QCCRID: 77903

Description: Unable to modify a virtual machine's storage with add and remove operations in the same job.

Platform: ESX, ESXi

Subsystem: Virtualization - UI

Symptom: The modify virtual machine action fails.

Resolution: Fixed.

QCCRID: 78017

Description: The `ManageEsx create` command fails with a Null Pointer Exception (NPE).

Platform: Linux/3AS, Linux/4AS, Linux/5Server, SunOS

Subsystem: Virtualization - API

Symptom: `ManageEsx` was originally written as a unit test. It did not work and was not documented. It was replaced with a shell script.

Resolution: Fixed.

QCCRID: 81233

Description: There is a Null Pointer Exception (NPE) when opening a scheduled Create/Modify/Remove virtual machine job whose server has been deleted.

Platform: Solaris, Vmware, HyperV

Subsystem: Virtualization - Other

Symptom: When you open Create/Modify/Remove virtual machine jobs whose server has been deleted, an NPE error displays.

Resolution: Fixed.

QCCRID: 81241

Description: A deleted hypervisor server is displayed as "null" in completed Create virtual machine and Remove virtual machine jobs.

Platform: Solaris, VMware, HyperV

Subsystem: Virtualization - Backend (VMware)

Symptom: In the server browser, "null" appears, instead of the server name if the server is deleted.

Resolution: Fixed.

QCCRID: 92213

Description: ESXi edit connection events should be logged in the history log file.

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: There is no edit connection event recorded in the history log for the hypervisor after the ESXi connection is modified.

Resolution: Fixed.

QCCRID: 92216

Description: Update ESX VMM code to version 2.5.

Platform: ESX, ESXi

Subsystem: Virtualization - Backend (VMware)

Symptom: SA should take advantage of latest enhancements and features such as cloning.

Resolution: Fixed.

QCCRID: 92336

Description: ESXi Edit connection: No HV scan is performed after a successful edit connection.

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: SA did not initiate a scan of the hypervisor after a successful edit connection. You must perform a reload data action.

Resolution: Fixed.

QCCRID: 93224

Description: A completed Create Virtual Zone job does not show the zone creation command script.

Platform: Solaris

Subsystem: Virtualization - UI

Symptom: The Create Virtual Zone job is run with a zone creation command script. When you open the completed job, the Zone Definition method shows "Filling a data form" instead of "Entering a zone creation command script".

Resolution: Fixed.

QCCRID: 93612

Description: Creating a virtual machine with multiple NICs causes OS provisioning to fail.

Platform: ESX 3, ESX 4, ESXi 3, ESXi 4

Subsystem: Virtualization - Backend (VMware)

Symptom: Creating a virtual machine with auto-provisioning and multiple NICs did not allow you to specify which NIC must be used as the provisioning device.

Resolution: Fixed. A new "Provisioning NIC" column is added to the table. This allows you to select a desired NIC out of N specified to perform the provisioning job.

QCCRID: 93686

Description: Suse64Guest is missing from the list of guests that require the E1000 adaptor.

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: Suse64Guest is excluded from the list of guests that require the E1000 adaptor.

Resolution: Fixed.

QCCRID: 93713

Description: Create Virtual Machine: The Job Status view is inconsistent between the live view and the view you get when opening the job from the history view.

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: The Job Status view is inconsistent between the live view and the job history view.

Resolution: Fixed.

QCCRID: 93764

Description: ESXi hypervisor in maintenance mode: You cannot create virtual machines when it is not allowed.

Platform: ESX 3, ESX 4, ESXi 3, ESXi 4

Subsystem: Virtualization - Backend (VMware)

Symptom: Hypervisors in maintenance mode that were the targets of any VMM operation would fail with an unrecognized error.

Resolution: Fixed.

QCCRID: 104418

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

Platform: ESX, ESXi

Subsystem: Virtualization - Backend (VMware)

Symptom: Hypervisors previously included in a device group, based on the OS property, would not be able to join the device group after VS registration.

Resolution: Fixed.

QCCRID: 105257

Description: "Network Name" and "VMware Guest OS" is not populated in the Virtual Machine Definition step after Modifying a virtual machine.

Platform: Independent

Subsystem: Virtualization

Symptom: There is no "Network Name" and "VMware Guest OS" information in the Virtual Machine Definition step after modifying a virtual machine.

Resolution: Fixed.

QCCRID: 108705

Description: Need a better error message when Run Custom Extension is attempted on vCenter managed ESX/ESXi servers.

Platform: Independent

Subsystem: Virtualization - Custom Extensions

Symptom: The error message is not clear when Run Custom Extension is attempted on vCenter managed ESX/ESXi servers.

Resolution: Fixed.

QCCRID: 109849

Description: When you add vCenter whose hypervisors are already managed by SA, the job fails with "integrity constraint (TRUTH.DEVICES_VSWITCH_INTERFACES_FK) violated - parent key not found".

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: Virtualization Service, which has SA managed ESX 3.0 hypervisors under management, failed with an error message.

Resolution: Fixed.

QCCRID: 109874

Description: Update ESXi credentials fails with a Null Pointer Exception (NPE).

Platform: VMware ESXi

Subsystem: Virtualization - Backend (VMware)

Symptom: In the Server browser Properties view, the user name appears as Username=<empty> and Credential Status=unverified for the ESXi hypervisor. Attempts to set the credentials results in an error (java NullPointerException).

Resolution: Fixed.

QCCRID: 110481

Description: Starting a managed Hyper-V virtual machine is logged in the SAS Web Client as "Start Zone".

Platform: Microsoft Hyper-V

Subsystem: Virtualization - Hyper-V

Symptom: Starting a Hyper-V virtual machine displays as a Job in the Web Client.

Resolution: Fixed.

QCCRID: 111307

Description: The add ESXi operation suspends on RHAS3 and RHAS4 cores.

Platform: VMware

Subsystem: Virtualization - Backend (VMware)

Symptom: Adding a hypervisor will suspend operation.

Resolution: Fixed.

QCCRID: 111363

Description: Modify VM fails when trying to modify/remove vlan adapter type VMXNET 2 or 3.

Platform: ESX, ESXi

Subsystem: Virtualization - Backend (VMware)

Symptom: Modify VM fails.

Resolution: Fixed.

QCCRID: 111775

Description: Debug information is logged in the twist stdout.log file.

Platform: VMware, Solaris

Subsystem: Virtualization - Backend (VMware)

Symptom: Debug information is displayed in a standard out file instead of in a log file.

Resolution: Fixed.

QCCRID: 111847

Description: A virtual machine is in a *powered on* state and you can add a disk but not change the size of the new disk or change the datastore after one is selected.

Platform: Independent

Subsystem: Virtualization - UI

Symptom: When a virtual machine is in a *powered on* state, you can add a disk but you cannot change the size of the new disk or the datastore after one is selected.

Resolution: Fixed.

QCCRID: 111922

Description: The create virtual machine job on an Agent managed ESX 3.5 fails with the error message: “com.vmware.vim25.VirtualMachineConfigSpec”.

Platform: ESX, ESXi

Subsystem: Virtualization - Backend (VMware)

Symptom: After a VMM upgrade, one file (from the previous installation) is not removed and causes failure.

Resolution: Fixed.

QCCRID: 111972

Description: The create virtual machine action fails on a managed ESX hypervisor when the virtual machine’s datastore name contains special characters.

Platform: ESX 3, ESX 4

Subsystem: Virtualization - Backend (VMware)

Symptom: Special characters, including blanks, in the controlling XML file caused argument passing to fail, resulting in ambiguous error messages and operation failure.

Resolution: Fixed.

QCCRID: 112176

Description: The Help button on the Add Hypervisor Progress window does not open the add hypervisor online Help topic.

Platform: Independent

Subsystem: Virtualization - UI

Symptom: The Help button on the Add Hypervisor Progress window does not open the add hypervisor Help topic; it opens the Server Automation User Guide Main Help.

Resolution: Fixed.

QCCRID: 112376

Description: The Power On, Power Off, Reset, Suspend, Modify, and Remove actions fail on virtual machines managed by ESX 3.05.

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: Several actions fail on virtual machines managed by ESX 3.05 (Power On, Power Off, Reset, Suspend, Modify, and Remove).

Resolution: Fixed.

QCCRID: 112417

Description: Modify VMware VM - Adding multiple hard disks to different datastores results in all disks being added to a single datastore.

Platform: ESX, ESXi

Subsystem: Virtualization - Backend (VMware)

Symptom: When you select multiple datastores, SA uses a single datastore for all entries.

Resolution: Fixed.

QCCRID: 112431

Description: Modify VMware virtual machine "Jobs and Sessions" displays "Power Status" as the virtual machine state.

Platform: Independent

Subsystem: Virtualization - UI

Symptom: In the Modify VM job, the State of the virtual machine shows "Power Status", instead of the correct state of the machine.

Resolution: Fixed.

QCCRID: 112733

Description: Hyper-V create virtual machine: You can select a value other than 8 MB RAM when a RAM value cannot be determined from the hypervisor.

Platform: Independent

Subsystem: Virtualization - Hyper-V

Symptom: When creating a Hyper-V virtual machine, you cannot enter any RAM value because the value was restricted to 8 MB.

Resolution: Fixed.

QCCRID: 113607

Description: The default window for modifying a virtual machine does not show the Size box when adding VHD in Storage Configuration.

Platform: Independent

Subsystem: Virtualization - Hyper-V

Symptom: During a virtual machine modification, when adding VHD, the File Location does not work for input without an ending backslash (\).

Resolution: Fixed.

QCCRID: 113659

Description: Modify VM - Virtual Machine Definition - When you add a description that includes the equals (=) character, it fails and displays the following error: "ValueError: too many values to unpack".

Platform: Windows 2008

Subsystem: Virtualization - Hyper-V

Symptom: An error is displayed when adding a description to the Virtual Machine Definition.

Resolution: Fixed.

QCCRID: 111590

Description: Incorrect history events are logged by failed, recurring, hypervisor scans.

Platform: Independent

Subsystem: Virtualization - Backend (VMware)

Symptom: The "Reload data for virtualization service failed" event should be logged.

Resolution: Fixed.

QCCRID: 111691

Description: The Virtualization panel displays a "java.lang.IndexOutOfBoundsException" and then the view panel goes blank.

Platform: Independent

Subsystem: Virtualization - UI

Symptom: Power on/power off for a virtual machine causes the Virtualization panel to display a blank page.

Resolution: Fixed.

Other

QCCRID: 109998

Description: Multimaster conflicts are created under very specific circumstances.

Platform: RHEL ES 3, SunOS 5.9

Subsystem: Core - Other

Symptom: Multimaster conflicts are created when creating OS Installation Profiles for RHEL ES 3 or SunOS 5.9 under very specific circumstances.

Resolution: Fixed.

QCCRID: 112878

Description: The pytz library is not usable from an APX due to root-only file privileges.

Platform: Independent

Subsystem: Core - Other

Symptom: APX authors are not able to use the pytz python library in their APXs because it fails to load due to file privilege issues.

Resolution: Fixed.

4 Known Problems, Restrictions, and Workarounds in SA 9.01

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



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

Agent Installer

QCCRID: 107917

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

Platform: Windows

Subsystem: Agent Installer

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

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

```
%SystemDrive%\Program Files\opsware\agent\lcpython15\Lib\site-packages\win32com\gen_py\
```

```
%TEMP%\gen_py
```

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

QCCRID: 111593

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

Platform: Windows

Subsystem: Agent Installer

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

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

Agents

QCCRID 100660

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

Platform: Windows Server 2008 using UAC

Subsystem: Windows Agent Deployment

Symptom: On Windows Server 2008, Windows ADT login fails for administrators that are not user Administrator due to Windows UAC controls used to secure the environment.

Workaround: Turn off UAC:

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

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

QCCRID: 110347

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

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

Platform: Windows

Subsystem: Agent

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

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

Application Configuration

QCCRID: 50099

Description: A script that includes Japanese characters in the filename and content fails with errors.

Platform: Windows

Subsystem: Application Configuration - Backend

Symptom: Execution of a data manipulation script that contains Japanese characters in its filename and content fails with errors.

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

QCCRID: 111765

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

Platform: Independent

Subsystem: Application Configuration

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

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

Application Deployment Manager

QCCRID: 110220

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

Platform: Independent

Subsystem: Application Deployment Manager

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

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

QCCRID: 110637

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

Platform: Independent

Subsystem: Application Deployment Manager

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

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

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

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

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

QCCRID: 111106

Description: Problems exporting ADM Environment to Device Group

Platform: Independent

Subsystem: Application Deployment Manager

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

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

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

QCCRID: 111925

Description: Configuration file installation requires that destination directory exists

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: A deployment that includes a Configuration File component fails without any warning or error when attempting to place a file in a directory that has not been created in advance.

Workaround: Ensure that a Code (or other type of ADM component) creates the destination directory in preparation for file placement by the Configuration File component.

QCCRID: 113202

Description: Installer should automatically add `truth.sid` to `da.conf`

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: The Application Deployment Manager fails to launch when a non-default Oracle System ID is used (SID is not "truth")

Workaround: To resolve the issue, perform the following steps:

- 1 Stop the Application Deployment Manager:
`/etc/init.d/opsware-sas stop da`
- 2 Add the `truth.sid` configuration parameter to `/etc/opt/opsware/da/da.conf` as in
`truth.sid=<newSIDname>`
- 3 Restart ADM service
`/etc/init.d/opsware-sas start da`

QCCRID: 115187

Description: The Application Deployment Manager does not work after upgrading from 7.8 to 9.0 in an Oracle Real Application Clusters (RAC) environment

Platform: Independent

Subsystem: Application Deployment Manager

Symptom: After upgrading from SA 7.8 to SA 9.x in an Oracle RAC environment, the Application Deployment Manager fails to launch

Workaround: Perform the following steps after the upgrade:

- 1 Run the following command to stop the Application Deployment Manager:
`/etc/init.d/opsware-sas stop da`
- 2 In the `/etc/opt/opsware/da/da.conf` file, remove the `truth.sid` configuration parameter. For example:
`truth.sid=<SIDname>`
- 3 Edit the following file:
`/opt/opsware/da/webapps/arm/WEB-INF/classes/hibernate.cfg.xml`
- 4 Locate the block that contains the `connection.driver` and `connection.username` properties.
- 5 Add the following string:

```
<property name="connection.url">jdbc:oracle:thin:@ (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = host1) (PORT = 1521)) (ADDRESS = (PROTOCOL = TCP) (HOST = host2) (PORT = 1521)) (LOAD_BALANCE = yes) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = truth) (FAILOVER_MODE = (TYPE = SELECT) (METHOD = Preconnect) (RETRIES = 180) (DELAY = 5))))</property>
```

Here, `host1` and `host1` are variables that represent the names of your database servers. Include one `(ADDRESS = (PROTOCOL = TCP) (HOST = hostname) (PORT = 1521))` specification for every database server in your environment.
- 6 Run the following command to restart the Application Deployment Manager:
`/etc/init.d/opsware-sas start da`

- 7 Re-run the Opsware Installer—or, alternatively, invoke the following command to populate the Application Deployment Manager baseline data:

```
/opt/opsware/da/bin/da_baseline.sh
```

Audit and Remediation

QCCRID: 102706

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

Platform: Independent

Subsystem: Audit and Compliance

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

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

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

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

BSA Essentials Dataminer

QCCRID: 112784

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

Platform: All

Subsystem: BSA Essentials Dataminer

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

Workaround: None.

Database Scanner for Oracle

QCCRID 88091

Description: Certain files (utility scripts) are not automatically removed from a managed server. These are Database Scanner for Oracle binaries that are copied to a managed server during each snapshot process.

Platform: Independent

Subsystem: Database Scanner for Oracle

Symptom: Each time you create a Database Scanner snapshot, you will see these files on the managed server because they are copied to it during the snapshot process.

Workaround: If you need to repurpose a managed server and it still has these files on it, you should remove them to *clean* the server. To remove all Database Scanner for Oracle binaries from a managed server, perform the following steps:

- 1 From the Navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**.
- 2 Right-click the managed server and then select **Run Script** ► **Select Script**.
- 3 In the Run Server Script window, click **Select Script** to display the Select Script dialog.
- 4 In either the Browser Scripts tab or the Browse Folders tab, select the "post-uninstall script for Database scanner for Oracle [unix | win]" script and then click **Select**.

To view this script, you must have privileges on the "/Opware/Tools/Server Modules com.opware.server.module.storage.dbscanner.oracle" folder.

- 5 In the Run Server Script window, click **Next** and then click **Start Job** in the Options pane. Do not specify any additional parameters.

When the job successfully finishes, all files related to the Database Scanner for Oracle will no longer be on the *cleaned* managed server.

QCCRID 91143

Description: The status of an ASM Diskgroup shown in the Properties view is different than the status shown in the Database Configuration Assistant (DBCA) view.

Platform: Independent

Subsystem: Database Scanner for Oracle

Symptom: In the Properties view, the status is CONNECTED. In the DBCA, the status is MOUNTED. By definition, the status of ASM Diskgroup is relative to the database instance. What is reported in the Properties view matches the status for one database instance only.

Workaround: None.

QCCRID 93690

Description: The Server ► Relationships ► SAN Switches panel only displays SAN switches to which the given server is directly connected. In some cases, a server may depend on SAN switches that are not displayed in this panel. For example, a virtual server may be using storage allocated from a hypervisor that was allocated storage from a SAN.

Platform: Independent

Subsystem: Database Scanner for Oracle

Symptom: The content pane for Relationships (SAN Switches and SAN Fabrics) on a virtual server is empty (“No items found”).

Workaround: None.

Bug ID: 156909 / QCCRID 68263

Description: Tablespace's free space view does not match the Oracle Enterprise Manager (OEM) view.

Platform: Independent

Subsystem: Database Scanner for Oracle

Symptom: In the tablespace view, the free space does not match what is displayed in the Oracle Enterprise Manager (OEM) tablespace.

Workaround: None

Note: There is an OEM bug about some tablespaces showing the incorrect used size. The Database Scanner for Oracle gets the tablespace used size directly from all of its data files, which avoid the OEM bug.

Installer

QCCRID 100931

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

Platform: Independent

Subsystem: SA Installer

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

```
Removing com.opsware.server.module.storage.compliance
This will probably take a long time.
[...]
Failed to remove ServerModule from servers
[...]
Failed to remove software policy 'Storage Compliance Checks' (8710001)
ProtocolError: <ProtocolError for 192.168.161.22/cogrpc.py: 404 Not found>
```

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

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


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

QCCRID 114639

Description: Installing a version 9.0 Slice Component bundle on a 9.xx patched core resets the wayscript versions to 9.0.

Platform: Independent

Subsystem: Installer

Symptom: If you install additional Slice Component bundle instances after patching the SA Core to version 9.xx, wayscript versions are set to version 9.0 rather than the patch version.

Workaround:

- 1 From the SAS Web Client, log in as administrator (opsware admin user) and navigate to **Environment > Customer > Opsware > Custom Attributes > CORD_OPswwayscripts**. Identify the SA core server by checking the value field of the custom attribute CORD_OPswwayscripts.
- 2 Log in to the SA Core server you identified in step 1 and execute the following commands:

```
cd /var/opt/opsware/OPswpatch/OPswwayscripts/scripts  
./post_after_startup.sh
```
- 3 Apply any required hotfixes to the wayscripts.

ISM Tool

QCCRID: 110511

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

Platform: Windows Server 2008

Subsystem: ISM Tool

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

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

Model Repository

QCCRID: 83813

Description: Attempting to synchronize a Multimaster Mesh conflict on a Service Instance fails.

Platform: All

Subsystem: Model Repository (truth)

Symptom: Attempting to synchronize a Multimaster Mesh conflict on a ServiceInstance fails with the error:

```
ERROR -- Unable to perform UPDATE!
spin.genericDatabase error: 'ORA-02291: integrity constraint (.) violated -
parent key not found
ORA-06512: at "TRUTH.SERVICE_INSTANCES_DVC_ID_RTRG", line 14
ORA-01403: no data found
ORA-04088: error during execution of trigger
'TRUTH.SERVICE_INSTANCES_DVC_ID_RTRG' during 'UPDATE service_instances SET
mod_dt = TO_DATE(:p1, 'DD-MON-YYYY HH24:MI:SS'), tran_id = :p2 WHERE
(srvc_inst_id = :p3)' with args '('20-OCT-2008 23:40:21', '124970002',
'3230002)'
```

Workaround: Run the patch script `patch_database.sh` ensuring that the file `optional_updates.conf` is configured as described in [Database Schema Update Procedure](#) on page 27 of these release notes.

QCCRID: 113314

Description: During secondary core creation and setup, an export of the primary core Model Repository has to be taken. The SA 9.0 Installer throws errors on the primary core when export of Model Repository is taken. A similar error is thrown on the secondary core when the Model Repository is imported.

Platform: All

Subsystem: Model Repository (truth)

Symptom: The following error is thrown by the OI during export or import of Model Repository:

```
ORA-39002: invalid operation
ORA-39070: Unable to open the log file.
ORA-29283: invalid file operation
ORA-06512: at "SYS.UTL_FILE", line 488
ORA-29283: invalid file operation
```

```
java.lang.Exception: Execution of /var/tmp/oitmp/
ti_script2294908527303438968.sh failed with exit status 1
[ERROR] Aborting.
Output log to /var/log/opsware/install_opsware/truth/
truth_install_1276642504797.log
[Jun-15-2010 22:56:46] Component installation script encountered an error
(exit status 1)
[Jun-15-2010 22:56:46] Exiting Opsware Installer.
```

Workaround: See [Adding a Secondary Core Using the SA 9.0 Installer in an Oracle RAC or Remote Database Environment](#) on page 138.

OS Provisioning

QCCRID: 100928

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

Platform: Red Hat Enterprise Server 5

Subsystem: OS Provisioning

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

Workarounds: The available workarounds are:

- 1 Do not deploy RAID policies captured with ACU Version: 8.35.7.0 (linux5 boot image). Instead you should perform captures with ACU Version: 8.25.5.0 (using boot images other than linux5) and deploy those.
- 2 Modify the `raid.hpacu.script` custom attribute value for RAID Array Configuration on ACU Version: 8.35.7.0-captured RAID policies to use the correct drive indexes. For example, modify this captured configuration:

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

to the following:

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

QCCRID 102830

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

Platform: Independent

Subsystem: OS Provisioning - OCC - Client

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

Workaround: None

QCCRID: 103362

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

Platform: Independent

Subsystem: OS Provisioning Backend

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

Workaround: None.

QCCRID: 103394

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

Platform: Red Hat Linux

Subsystem: OS Provisioning Backend

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

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

QCCRID: 103602

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

Platform: Windows

Subsystem: OS Provisioning Backend

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

Workaround: None.

QCCRID: 104194

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

Platform: Independent

Subsystem: OS Provisioning Backend

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

```
Exit status: 1280
```

Error message from ACU: ERROR: (2821) No controllers detected.

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

QCCRID: 104739

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

Platform: Red Hat Enterprise Server IA64

Subsystem: OS Provisioning

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

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

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

QCCRID: 109044

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

Platform: Windows

Subsystem: OS Provisioning Backend

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

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

QCCRID: 109077

Description: Assign Customer OS Build Plan content script fails on customer names containing certain punctuation characters.

Platform: Windows

Subsystem: OS Provisioning Backend

Symptom: Quote characters in customer names are not supported.

Workaround: When creating an OS Build Plan, if the customer name contains quote characters, you must specify the customer ID instead of the actual customer name.

QCCRID: 110563

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

Platform: Windows

Subsystem: OS Provisioning Backend

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

Workaround: Use only ASCII characters where possible.

QCCRID: 111245

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

Platform: Independent

Subsystem: OS Provisioning

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

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

QCCRID: 111337

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

Platform: Solaris

Subsystem: OS Provisioning

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

Workaround: None.

QCCRID: 111445

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

Platform: Independent

Subsystem: OS Provisioning

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

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

QCCRID: 114523

Description: When performing OS provisioning using Application Deployment Automation, if the SA OS Sequence in use includes a device group and multiple servers are provisioned simultaneously, some of those server provisioning jobs will fail with an error. The error message will include "Unexpected general exception: com.opsware.device.DeviceGroupVO.modifiedDate is set to the illegal value".

Platform: Linux, Solaris, Windows

Subsystem: OS Provisioning

Symptom: OS Provisioning fails with the error message: "Unexpected general exception: com.opsware.device.DeviceGroupVO.modifiedDate is set to the illegal value".

Workaround: Do not include any device groups in your OS Sequence.

QCCRID: 111781

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

Platform: Windows Server 2003

Subsystem: OS Provisioning Backend

Symptom:

- When provisioning Windows Server 2003 or 2008 using an OS Sequence to a non-C drive using a WIM image:
 - Windows Server 2003 OS Media: *works*
 - Windows Server 2003 WIM: *fails*
 - Windows Server 2008 OS Media and WIM: *fails*
- When provisioning Windows Server 2003 or 2008 using an OS Build Plans to non-C drives:
 - Windows 2003 & 2008 OS Media installs: *supported*
 - Windows 2003 & 2008 WIM installs: *Unsupported*

Workaround: None

QCCRID: 111845

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

Platform: Red Hat Linux

Subsystem: OS Provisioning - MBC

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

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

QCCRID: 115063

Description: After migration, Windows Server 2008 R2 x64 servers are listed as Windows Server 2008 x64 in the SAS Web Client but correctly as Windows Server 2008 R2 x64 in the SA Client.

Platform: Windows Server 2008 R2 x64

Subsystem: OS Provisioning

Symptom: Migrated Windows Server 2008 R2 x64 servers are labeled incorrectly in the SAS Web Client.

Workaround: None

QCCRID: 116936

Description: Not all migrated Windows Server 2008 R2 x64 servers are moved to Public/Opware/All Windows/Windows Server 2008 R2 x64.

Platform: Windows Server 2008 R2 x64

Subsystem: OS Provisioning

Symptom: If you migrate a Windows Server 2008 x64 server but do not use the `-- listmrls` and `--mrl=<MRL_ID>` option to migrate any attached OS Sequences and associated Patch Policies and/or Software Policies, irreversible data integrity errors occur.

Workaround: None

Patch Management for Solaris

QCCRID: 98409

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

Platform: Solaris

Subsystem: Patch Management - Solaris

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

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

QCCRID: 100566

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

Platform: Solaris

Subsystem: Patch Management - Solaris

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

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

QCCRID: 109142 and 115536

Description: The default Solaris patch configuration file is overwritten when upgrading to SA 9.xx. The Solaris patch configuration file is used by the `solpatch_import` command and is located at `/etc/opt/opsware/solpatch_import/solpatch_import.conf`.

Platform: Solaris

Subsystem: Patch Management - Solaris - Backend

Symptom: If you have modified the default Solaris patch configuration file and you upgrade to SA 9.xx, your changes to the configuration file will be overwritten.

Workaround: Save your modified Solaris patch configuration file before performing the upgrade to SA 9.xx. After the upgrade, update your Solaris patch configuration file and run `./solpatch_import -a update_supplements`.

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

QCCRID: 109359 and 109361

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

Platform: Solaris

Subsystem: Patch Management - Solaris - Backend

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

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

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

Method 1 - Remove Solaris bundles using the SA Client.

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

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

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

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

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

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

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

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

- 3 Complete the upgrade to SA 9.0.
- 4 Create a new Solaris patch database using the following command:

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

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

QCCRID: 111342

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

Platform: SunOS 5.6 - 5.10 and SunOS 5.10 x86

Subsystem: Patch Management - Solaris

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

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

QCCRID: 114156

Description: Users with an existing metadata database (`solpatchdb`) must delete the `solpatchdb.zip`, `solpatchdb-old.zip` and `solpatchdb_supplement.zip` files and run `create_db` to have support for recommended obsolete patches.

Platform: Solaris

Subsystem: Patch Management - Solaris

Symptom: The `solpatch_import -filter` option does not display recommended and/or security patches if they had previously been marked obsolete. This became an issue on June 4, 2010 when Oracle changed the criteria for recommended and security patches (described here: http://blogs.sun.com/patch/entry/merging_the_solaris_recommended_and).

Workaround: You must recreate the Solaris patch metadata database (`solpatchdb`) if the following are true:

- 1 You use the `solpatch_import -filter` option.
- 2 You have run `solpatch_import -update_db` on June 4, 2010 or later.

After you have installed SA 9.01, perform these tasks to recreate the metadata database (`solpatchdb`):

- 1 Log in to the SA Client.
- 2 Select Library in the Navigation pane.
- 3 Select By Folder.

- 4 Navigate to /Opware/Tools/Solaris Patching.
- 5 Delete the following files:
 - solpatchdb.zip
 - solpatchdb-old.zip
 - solpatchdb_supplement.zip

Follow the steps to create a new metadata database (solpatchdb) as described in the *SA User Guide: Application Automation, Patch Management for Solaris*.

Patch Management for Windows

QCCRID: 102713

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

Platform: Windows

Subsystem: Patch Management - Windows - Backend

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

Workaround: None.

QCCRID: 108451

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

Platform: Windows Server 2008 x64

Subsystem: Patch Management - Windows - Backend

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

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

QCCRID: 105098

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

Platform: Windows

Subsystem: Patch Management - Windows - Backend

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

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

QCCRID: 110257

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

Platform: Windows Server 2008 x86

Subsystem: Patch Management - Windows - Backend

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

Workaround:

- 1 To install these patches, import the April 2010 (or later) version of the BSA Essentials Network patch supplement from the BSA Essentials Network on to your SA core server.
- 2 Visit <http://support.microsoft.com/kb/980966/> to download KernelSystemStateCheck.exe to determine whether the patch can be installed on your Windows Server 2008 (x86) managed servers.
- 3 Contact HP Server Automation Support in order to get this file “qc110257.pyc”. (The Quality Center bug report number is QCCRID 110257.)
- 4 On the SA core, copy qc110257.pyc to the SA core’s Data Access Engine (spin) server.
- 5 As root on the SA Data Access Engine (spin) server, execute the following command:

```
# /opt/opsware/bin/python2 qc110257.pyc
```
- 6 Assuming Microsoft's KernelSystemStateCheck.exe utility reports a pass result, use the ad-hoc Install Patch task window to install the version of MS10-015 (KB977165) that has a file name of Windows6.0-KB977165-x86.msu, and the version of MS10-021 (KB979683) that has a file name of Windows6.0-KB979683-x86.msu.

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

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

QCCRID: 110471

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

Platform: Windows Server 2008 x86

Subsystem: Patch Management - Windows - Backend

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

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

QCCRID: 111397

Description: When the vendor recommended patch policy is remediated on a Windows managed server, depending on what patches were applied, the server may require the vendor recommended patch policy to be remediated again. This can happen when older patches are applied during the first remediate. If an older patch introduces problems fixed by newer patches, SA detects this only after the older patch is installed; therefore, a second remediate is required to address the problem.

Platform: Windows

Subsystem: Patch Management - Windows - Backend

Symptom: After remediating the vendor recommended policy on a Windows managed server, the server's recommended patch list shows additional patches that need to be installed therefore requiring the vendor recommended policy to be remediated again.

Workaround: None.

SA Client (Framework)

QCCRID:105671

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

Platform: Windows

Subsystem: SA Client Framework

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

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

SA Client (Search)

Bug ID: 155094 / QCCRID 66448

Description: Advanced Search results for Storage System Discovery Date do not display correctly.

Platform: Independent

Subsystem: SA Client (Search)

Symptom: If the user profile setting on the SAS Web Client is UTC, all discovered dates will display as expected. If the user profile setting is set to a timezone other than UTC, some discovery dates for SAN arrays, NAS filers, and switches will not display as expected, although they are technically correct.

SA/NA Integration

QCCRID:90653

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

Platform: Independent

Subsystem: SA/NA Integration

Symptom: SA/NA Integration fails.

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

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

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

SA/OO Integration

QCCRID:102614

Description: Before integrating SA with any HP Operations Orchestration (OO) flows using the SA Client, you must import the OO SDK Client certificate. Make sure that the version of the OO SDK Client Certificate is compatible with the version of OO you plan to use with SA. Typically, you can import the certificate once and the same OO SDK Client Certificate will support different versions of OO. SA 9.01 contains an OO SDK Client Certificate for OO version 7.51, which also supports OO versions 7.6 and 9.0. See the *SA Integration Guide* for information on how to import the OO SDK Client Certificate.

Platform: Independent

Subsystem: SA/OO Integration

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

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

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

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

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

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

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

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

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

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

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

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

Example output:

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

- 6 Enter the following command to start the twist:

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

SA/SAR Reports

QCCRID: 105234

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

Platform: Independent

Subsystem: SA Client Reporting

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

Workaround: Run the report using the following parameters:

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

QCCRID: 107293

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

Platform: Independent

Subsystem: SA Client Reporting

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

Workaround: None.

QCCRID: 112434

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

Platform: Independent

Subsystem: SA Client Reporting

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

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

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

```
su - omdb
```

- 3 Enter the following commands:

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

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

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

Example:

```
<folder name="reports">
<display_name>Reports</display_name>
<folder_reports></folder_reports>
<subfolders>
<subfolder_name>application_deployment_reports</subfolder_name>
<subfolder_name>top_level_patch_reports</subfolder_name>
.....
.....
</subfolders>
<parent>none</parent>
</folder>
```

- 5 Save the `report_def.xml` file.
- 6 Launch the BSA Essentials Java Client.
- 7 Click on the Reports folder to see the “Application Deployment” folder and “Patch” folders.

SAS Web Client

QCCRID: 109000

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

Platform: Any

Subsystem: SAS Web Client

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

Workaround: There are two solutions to this issue:

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

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

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

2. Disable IE ESC altogether.

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

Satellites

QCCRID: 97659

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

Platform: Windows

Subsystem: Satellites

Symptom: Network scans fail with an error.

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

Script Execution

QCCRID: 79545

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

Platform: Windows

Subsystem: Script Execution

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

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

SE Connector

QCCRID 88755

Description: There is no Target and Target Volume information displayed for a LUN.

Platform: Independent

Subsystem: SE Connector

Symptom: Target and Target Volume display "-" for a LUN in the storage volume access path view.

Workaround: None.

QCCRID 91582

Description: Provisioning changes on a volume or pool for an EVA array might not immediately display in its corresponding Inventory view.

Platform: Independent

Subsystem: SE Connector

Symptom: When you perform a provisioning operation for an HP EVA array (such as create, delete, or

modify a volume or pool), the changes for the volume or pool might not be immediately available in SA after running the "Update from Storage Essentials" process.

Workaround: After 30 minutes has lapsed, run the "Update from Storage Essentials" process again. See the Storage Essentials SRM Software User Guide for information about provisioning EVA arrays.

QCCRID 105778

Description: After deploying SE Storage Scanner on a few hosts, select Administration ► Storage Scanners ► <The names of the SE Scanner on "Host"> The Host name is missing on some of them.

Platform: Independent

Subsystem: SE Connector

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

Workaround: Manually delete the inactive Storage Scanner entries from the Storage Scanner panel by using the Remove menu option provided for each entry.

Server Automation Installer

QCCRID: 111215

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

Platform: SUSE Enterprise Linux 9

Subsystem: Installer

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

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

<distro>/opsware_installer/tools/restore_stage2.pyc

Software Management

QCCRID: 100754

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

Platform: All

Subsystem: Software Management

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

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

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

Workaround: None

QCCRID: 101517

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

Platform: All

Subsystem: Software Management

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

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

QCCRID: 102564

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

Platform: Solaris

Subsystem: Software Management - API - Compliance

Symptom:

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

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

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

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

QCCRID: 102934

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

Platform: Independent

Subsystem: Software Management - API - Compliance

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

Workaround: Increase the cache size.

QCCRID: 111356

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

Platform: Independent

Subsystem: Software Management - API - Software Policy

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

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

QCCRID: 115665

Description: Issues when migrating software policies attached to dynamic groups with the rule `Operating System=Windows 2008 x64` specified.

Platform: Windows Server 2008 R2 x64

Subsystem: Software Management - Tools - Migration

Symptom: Migrating a Windows Server 2008 R2 x64 server, attached to a dynamic device group with the rule `Operating System=Windows Server 2008 x64` specified, prevents all Application Configurations, remediated using a Software Policy, from being detached from the server.

Workaround: None

Storage Host Agent Extension

QCCRID 93630

Description: On Windows servers that have EMC PowerPath installed as the multipathing software, the SCSI Bus number provided by PowerPath (using the `powermt` command) does not match the bus number of the disks (LUNs). In these cases, LUNs are displayed as "ROOT" and display alongside LUNs that are correctly displayed.

Platform: Windows

Subsystem: Storage Host Agent Extension

Symptom: LUNs that are multipathed by EMC PowerPath are shown as both "ROOT" and "LUN" in the Inventory ► Storage ► Volumes Panel.

Workaround: None.

QCCRID 105382

Description: On Windows 2008, if the disk information is changed, such as presenting new LUNs or removing existing LUNs, running the storage snapshot specification results in incorrect capacity values shown in the Inventory ► Storage ► Disk panel. This occurs if there is a mismatch in the disk names, as reported by the hardware registration script and the storage snapshot specification.

Platform: Windows

Subsystem: Storage Host Agent Extension

Symptom: Disk capacity shown in the Inventory ► Storage ► Disk panel is incorrect.

Workaround: To resolve this issue, after changing disk information (such as installing or uninstalling multipathing software, presenting new LUNs, deleting LUNs, and so on) on the Windows managed server, the server must be rebooted. Run the hardware registration before running the storage snapshot specification.

QCCRID 105953

Description: An EMC Symmetrix array that is discovered through SE Connector can report more than one storage volume with the same LUN number presented to a managed server. Running the storage snapshot specification on the managed server will succeed; however, the Inventory ► Storage ► File Systems and Inventory ► Storage ► Managed Software panels will be empty.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: The Inventory ► Storage ► File Systems and Inventory ► Storage ► Managed Software panels will be empty. Also, some host volumes with a LUN service type will not be displayed in the Storage ► Inventory ► Volumes panel. For the EMC storage array in the Relationships ► Storage Initiators panel for this managed server, there will be more than one volume that has the same LUN number.

Workaround: None.

QCCRID 106400

Description: For AIX managed servers, if there are stale disks (LUNs) present on the server, the supply chain and composition information is not properly displayed. For some of the volumes, the composition information may not be present.

Platform: AIX

Subsystem: Storage Host Agent Extension

Symptom: For the AIX servers, under Inventory ► Storage ► Volumes, for some of the volumes created out of LUNs, the right hand lower panel will not show the Composition and/or Connectivity information.

Workaround: Delete the stale volumes on the AIX managed server and run the storage inventory snapshot specification.

QCCRID 106699

Description: For Windows 2008 managed servers with mirrored volumes, if one of the disks that is part of a mirrored volume fails or is removed, the state of the volume is shown as "Failed Redundancy" in the Disks Management panel on the Windows server. However, in the Inventory ► Storage ► Volumes panel for the managed server, the status of this volume is shown as "OK", even after running storage snapshot specifications.

Platform: Windows 2008

Subsystem: Storage Host Agent Extension

Symptom: Status of mirrored volumes is shown as "OK" in the Inventory ► Storage ► Volumes panel, even if one of the disks that is part of the mirrored volume fails or is removed.

Workaround: None.

QCCRID: 107944

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

Platform: VMware ESX 3.0.x

Subsystem: Storage Host Agent Extension

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

Workaround: None.

QCCRID 109306

Description: On Linux, the supply chain breaks when users create multilevel LVM RAID volumes, such as RAID10 or RAID50, and the Inventory ► Storage ► Volumes panel does not display supply chains for multilevel-RAID volumes.

Platform: Linux

Subsystem: Storage Host Agent Extension

Symptom: The Inventory ► Storage ► Volumes panel does not display supply chains for multi-level RAID volumes.

Workaround: None.

QCCRID 111724

Description: The Storage Host Agent Extension does not support virtual servers that have VMDK created on NFS datastore.

Platform: All VMware servers

Subsystem: Storage Host Agent Extension

Symptom: Host Storage Inventory will fail on VMware servers that have VMDK on NFS datastore. Therefore, no storage information will be collected on VMWare servers with this configuration.

Workaround: None.

QCCRID 111727

Description: Storage Host Agent does not support virtual servers that have VMDK created on the NFS datastore.

Platform: All VMware servers

Subsystem: Storage Host Agent Extension

Symptom: The host storage inventory will fail on VMware servers that have VMDK created on the NFS datastore. Therefore, no storage information will be collected on VMware servers with this configuration.

Workaround: None.

QCCRID 116264

Description: There are multimaster conflicts in AIM_FIBRE_CHANNEL_ADAPTER.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: When a managed server (that previously had Storage Host Agent Extension installed for collecting Fibre Channel Adapter data) is not deactivated and deleted from a multimaster core before managing the same server again, the old data will cause conflicting records between the cores. These conflicts are caused by the FCA card data of the managed server that has different OID's with the same external key. When you perform a forced uninstallation of the SA Agent from a managed server, add the server back to the core without first deleting the old server data from the core, deploy the Storage Host Agent Extension, and collect the FCA data, conflicts will be generated.

Workaround:

- 1 In the SA Client, select **Deactivate Server** ► **Delete Server** to deactivate and delete the managed server from the core.
- 2 Log on to the managed server and manually uninstall the SA Agent. See *SA User's Guide: Server Automation*, Appendix B, "Uninstalling an Agent on Unix and Windows".
- 3 Remove the following folders on the server.

```
/opt/opsware  
/etc/opt/opsware  
/var/opt/opsware
```
- 4 Add the managed server back to the core.
- 5 Clear the conflicts. See the *SA Administration Guide*, Chapter 3, "Multimaster Mesh Conflict Administration", for information about "Best Practices for Resolving Database Conflicts".

QCCRID 116775

Description: Managed servers with Storage Host Agent, Inventory ► Disks sometimes shows storage LUNs and local disks when only local disks should be displayed.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: For a managed server, generate a Server Storage Inventory snapshot. Open the managed server browser and select Inventory. Open the Storage ► Disks option in the left pane. Only local disks should display; however, on some servers, all LUNs and disks are displayed.

Workaround: None.

Bug ID: 149406 / QCCRID 60760

Description: Solaris LVM RAID on Soft Partition on slices stops responding.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: This configuration produces a defective storage supply chain.

Workaround: None

Bug ID: 149707 / QCCRID 61061

Description: The Storage Host Agent Extension reports two single port cards when a single dual port card is present.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: The SNIA v1 HBA API reports ambiguous information with regard to ports on a multi-port card. Some vendors may model dual port cards as two single-port cards. This is the information that ASAS reports on—output that shows a single dual port card with a single serial number, where each adapter has its own unique node WWN.

Workaround: None

Bug ID: 151921 / QCCRID 63275

Description: There is no distinction between the volume types “Mirror Concatenated” and “Mirror Striped” in the Volume Manager labels.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: When you add a mirror to concatenated or stripe, the volume display labels both as “Mirrored” and does not distinguish between concatenated or striped in the label. Note that “Mirrored Concatenated” and “Mirror Striped” are distinct on the volume manager on the host, such as on the Veritas Volume Manager.

Workaround: None. The type of volume manager might not match the native tool, such as the Veritas Volume Manager. The `STORAGE_TYPE` value is the immediate node in the supply graph, which is the storage type of the most decendent volume.

Bug ID: 152016 / QCCRID 63370

Description: The `STORAGE_DRIVE` value is incorrectly formatted for SunOS 5.10 disks.

Platform: Unix

Subsystem: Storage Host Agent Extension

Symptom: The value stored in `STORAGE_COMPONENTS.STORAGE_DRIVE` is a different format on Solaris 5.10 than on Solaris 5.8 and 5.9. The different format for 5.10 causes a broken storage supply chain on affected servers.

Workaround: Check the version number in the `/etc/format.dat` file on the server. If it is less than 1.28, update the file.

Bug ID: 152942 / QCCRID 64296

Description: QLogic 9.1.4.15 HBAAPI is defective.

Platform: Windows

Subsystem: Storage Host Agent Extension

Symptom: On a Windows 2003 server with the SNIA library from QLogic, Fibre Channel Adapter and storage volume information might not be discovered by the Storage Host Agent Extension, causing `fibrepoxxy.exe` to stop responding.

Workaround: For Windows Server 2003 and Microsoft Windows 2000 operating systems, use the native Microsoft SNIA library instead of the SNIA that is provided by the QLogic driver. Download the Fibre Channel Information Tool to add the Microsoft HBAAPI support to the operating system. For Windows 2003 SP1 or later, the Microsoft HBAAPI support is built in. If the SNIA's version of `hbaapi.dll` is installed on the operating system, remove it.

Bug ID: 154418 / QCCRID 65772

Description: The Unix QLogic snapshot is missing information in the Hardware view and Volumes pane.

Platform: Unix

Subsystem: Storage Host Agent Extension

Symptom: When you snapshot a Unix server that has a QLogic driver installed, there is no FC adapter information in the Hardware view. There is also no composition and connectivity information for any SAN volume in the Volumes pane.

Workaround: Install patches 108434 and 108435 on Solaris 8 SPARC servers. The Storage Host Agent Extension on Solaris 5.8 SPARC requires these patches.

Note: There is no known workaround for Red Hat 3 or Red Hat 4 servers using QLogic controllers.

Bug ID: 154971 / QCCRID 66325

Description: Veritas Storage Foundation 4.3 with QLogic 9.1.4.15 results in invalid fibre proxy SCSI addresses.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: The SAN storage volume displays both LUN and Root as the Service Type. There are two lines for the physical drives: One line displays LUN and the other displays Root.

Workaround: None

Bug ID: 155476 / QCCRID 66830

Description: There is no support for mounting Windows 32 file systems on non-drive letter locations.

Platform: Windows

Subsystem: Storage Host Agent Extension

Symptom: The file system is not shown on the server storage file system panel when the partition and format on the Windows server is mounted to an empty NTFS folder.

Workaround: None

Note: The Storage Host Agent Extension does not report file systems that have non-drive letter mount points. The Storage Host Agent Extension does not report file systems that have multiple mount points.

Bug ID: 157044 / QCCRID 68398

Description: Fibreproxy is broken on Windows 2000 SP4 server with a QLA2310 HBA and vendor driver version 9.1.4.10.

Platform: Windows

Subsystem: Storage Host Agent Extension

Symptom: A storage inventory snapshot does not gather and supply complete data, including storage volume and FCA information.

Workaround: None

Bug ID: 157579 / QCCRID 68933

Description: Running fibreproxy on a Windows server with Emulex installed returns multiple FibreChannelTargetMappings.

Platform: Windows

Subsystem: Storage Host Agent Extension

Symptom: When you run take a Storage Host Agent Extension snapshot by running fibreproxy on a Windows server where Emulex LP850, LP952, LP9002, or LP9402 is installed, three FibreChannelTargetMappings are returned, two of which are duplicates. This symptom does not occur with Emulex driver 1.30a9.

Workaround: None

Bug ID: 158923 / QCCRID 70277

Description: Disabling all MPIO paths for a device causes `diskproxy` and `mpioproxy` to stop responding.

Platform: AIX

Subsystem: Storage Host Agent Extension

Symptom: If you run the `chpath` command as shown below to take a Storage Host Agent Extension snapshot for each available path to the device, all the MPIO paths to a logical device become disabled. In this state, the system calls used by the `diskproxy` and `mpioproxy` will stop responding.

```
chpath -l hdisk2 -p fscsi0 -s disable xx
```

Workaround: None

Bug ID: 159156 / QCCRID 70510

Description: After you remove a LUN mapping, the old LUN mapping information still displays in the SAN array volume view and in the server storage volume view. An additional access path is displayed in the SAN array volume view (Access Path subview) for the volume for which LUN mapping was removed. The access path that shows no initiator device and/or initiator port information is the correct one.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: For a mounted SAN volume on a server, when LUN mapping for the same SAN volume on the storage array is updated to remove the initiator ports, the server still reports that it sees the volume. As a result, an incorrect access path for the SAN volume is displayed. The Storage Agent for the storage array correctly updates the LUN mapping when the next synchronization is run and shows no initiator ports for the LUN mapping. The incorrect access path is removed from the display when the next Storage Host Agent Extension snapshot is run.

Workaround: Take a snapshot of the server to which the volume was mapped or partitioned.

Bug ID: 159580 / QCCRID 70934

Description: SAV displays incorrect information after adding a zone to a fabric.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: A fabric zone to card WWN does not correlate to the server, but a zone to the port WWN does have correct correlation. The zone is not associated to the correct server/port/WWN.

Workaround: None

Bug ID: 164951 / QCCRID 76305

Description: Multipath information does not display correctly for an HP-UX 11iv2 server in the SA Client.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: The multipath information is not reported correctly for a server that has HP-UX 11iv2 OS installed and Veritas DMP managing the multipathing in the SA Client. The SNIA library does not support HBA_GetFcpTargetMappingsV2r.

Workaround: None

Bug ID: 168716 / QCCRID 80070

Description: Broken supply chain on AIX 5.2 with Powerpath.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: On servers running AIX 5.2 with PCI-X Fibre Channel Adapters, the supply chain does not display after taking an inventory snapshot.

Workaround: None

Bug ID:168889 / QCCRID 80243

Description: Logical volume devices appear to be under Veritas DMP control when they are not taking a new snapshot.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: If you disable a volume in Veritas DMP and subsequently take a new Storage Host Agent Extension snapshot, the updated volume appears as though it remains managed by Veritas DMP.

Workaround: When constructing LVM modules on the HP-UX 11.31 platform, use agile DSF devices. There is no workaround for other platforms.

Bug ID: 167103 / QCCRID 78457

Description: The Storage Disk panel appears empty after upgrading to SA 7.50 and ASAS 7.50.

Platform: Independent

Subsystem: Storage Host Agent Extension

Symptom: If you perform a core upgrade to SA 7.50 and ASAS 7.50 and then run the customer extension to upgrade a Storage Host Agent Extension on the host, the host disappears from the INTERFACE table and the host's STORAGE_DRIVE does not appear in the STORAGE_COMPONENT table.

Workaround: It may take one to two hours for the host and drives to repopulate their tables. Verify that the host is present in the `INTERFACE` table and that the `STORAGE_DRIVE` element is present in the `STORAGE_COMPONENT` table.

Virtualization

QCCRID: 90019

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

Platform: Windows Server 2008/Hyper-V

Subsystem: Virtualization

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

Workaround: Do not use duplicate virtual network names.

QCCRID: 106085

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

Platform: Windows Server 2008 pre-R2 server

Subsystem: Virtualization - Hyper-V

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

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

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

An icon for the pre-R2 server will appear in Hyper-V Manager.

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

8 Click **OK**.

QCCRID: 104418

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

Platform: VMware ESX (all versions)

Subsystem: Virtualization - Backend (VMWare)

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

Workaround: None.

QCCRID: 105999

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

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

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

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

QCCRID: 106909

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

Platform: Windows

Subsystem: Virtualization

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

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

QCCRID: 109887

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

Platform: Red Hat Linux

Subsystem: Virtualization

Symptom: Snapshot view is not available for ESX managed servers

Workaround: Manage ESX directly snapshot view.

QCCRID: 110035

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

Platform: VMWare ESXi

Subsystem: Virtualization

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

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

QCCRID: 111307

Description: The “add ESXi” operation suspends processing.

Platform: ESXi

Subsystem: Virtualization - Backend (VMWare)

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

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

QCCRID: 111789

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

Platform: Independent

Subsystem: Virtualization - Backend (VMWare)

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

Workaround: Add the vCenters separately.

QCCRID: 111922

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

Platform: ESX 3.5

Subsystem: Virtualization - Backend (VMWare)

Symptom: The Create Virtual Machine operation fails.

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

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

- 1 Create a script.
 - a From the Navigation pane, select **Library** ► **By Type** ► **Scripts** ► **Unix**.
 - b From the Actions menu, select **New** and then enter the following information:
Name: Clean VMM on ESX
Location: Select **Package Repository** ► **All VMWare Linux** ► **VMWARE ESX Server** <any version>
Script Content:

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



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

QCCRID: 111972

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

Platform: ESX

Subsystem: Virtualization - Backend (VMWare)

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

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

QCCRID: 116276

Description: After an SA Agent is installed and before hardware registration has completed, you can create or modify a virtual machine with a memory value that is larger than the hypervisor's physical memory.

Platform: Windows 2008, Windows 2008 R2

Subsystem: Virtualization - Hyper-V

Symptom: Install an Agent on a hypervisor Windows server. When the hardware information is not fully populated on the server, try to create a virtual machine or modify a virtual machine with a memory value that is greater than the maximum memory allowed on the hypervisor. The job successfully completes.

Workaround: Run a full hardware registration on the Windows server. After hardware registration is completed, SA will not allow you to use memory that is greater than the maximum memory allowed on a virtual machine for the actions to create and modify a virtual machine.

QCCRID: 116983

Description: Failed Clone VM jobs may cause data integrity errors from system diagnostics.

Platform: Independent

Subsystem: Virtualization

Symptom: If Clone VM completes the clone operation but fails to register the server, there may be a data integrity error from system diagnostics.

Workaround: Fix any networking problems and restart the cloned VM so that the SA agent completes registration.

Web Services Data Access Engine

QCCRID: 111039

Description: Out-of-memory error.

Platform: Red Hat Linux/Solaris

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

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

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

QCCRID: 112222

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

Platform: Red Hat Enterprise Linux AS3 32-bit

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

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

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

Workaround: Before upgrading, edit the file:

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

and add the following entry:

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

The value must be 2000 megabytes or less.

Example: `twist.mxMem=1960m`

5 Documentation Errata


This chapter contains information that corrects or updates the Server Automation Online Help and product manuals.



To check for updates, go to <http://support.openview.hp.com/selfsolve/manuals>. This site requires that you register for an HP Passport and sign in. To register for an HP Passport, select the **New users - please register** link on the HP Passport login page.

Application Deployment Manager Context-sensitive (F1) Help

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

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

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

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

SA 9.0 Single-Host Installation Guide

Create a User Account with Administrator Privileges (Page 15)

All occurrences of the user *Administrator* should be replaced with the user *System Administrator*.

Step 5 should read:

5. Under User Privileges: Group Membership, select the System Administrators user group.

SA 9.0 Simple/Advanced Installation Guide

The following changes affect the version 9.0 *SA Simple/Advanced Installation Guide*, Chapter 2: System Requirements. The following entries should be added to Table 16 (page 32):

Table 16: Open Ports on a Firewall Protecting an SA Core

Source	Destination	Open Port(s)	Notes
Management Desktops	Slice Component bundle hosts	80, 443, 8080	Required
Direct access to Oracle database (reports, troubleshooting, management)	Model repository (truth) host	1521	Strongly recommended to allow Oracle management
Management Desktops	Slice Component bundle hosts	1004, 1018, 1032, 2222	[Optional] Useful for troubleshooting; ports represent spin, way, twist, and ogsh (ssh).
SA Core (Management Gateway)	SA Core (Management Gateway)	2001	Required
SA Core (Management Gateway)	SA Core in a different Multimaster Mesh (management gateway)	22, 2003	[Optional] For scp (default word replication, can be forwarded over 2001 connection), backup for 2001 if it is busy.
Slice Component bundles	SA Agents (in same network)	1002	Required (only for the Agent Gateway managing the Agent).
SA Core (Management Gateway)	Satellite/Gateway	3001	Required
SA Core hosts	Mail server	25	Required for email notifications
SA Core hosts	LDAP server	636	Required for secure LDAP access; port can change if you use unsecure LDAP.
SA Agents	SA Core servers and Satellites managing the agent	3001	Required
SA Satellite/Gateway	SA Core	2001	Required
SA Satellite/Gateway	Managed Agents	1002	Required

Source	Destination	Open Port(s)	Notes
BSAe Core	Mail Server	25	Required for email notifications
BSAe Core	SA Core	1032	Required
BSAe Core	BSAe database	1521	Required
BSAe Desktop	SA Core	443	Required
BSAe Desktop	BSAe Core	8080,8443, 14445	Required
Data Miner (SA Core)	BSAe Core	8443, 8873	Required

SA 9.0 Simple/Advanced Installation Guide and Oracle Setup for the Model Repository

The following changes have been made to the *SA Simple/Advanced Installation Guide* and to the *Oracle Setup for the Model Repository* document, *Vault.conf File Changes* section (page 196):

The content that reads (note that the first entry **truth.sid=** is changed to **truth.sid:**):

```
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))))
```

is changed to read:

```
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))))
```

SA 9.0 Simple/Advanced Installation Guide and Oracle Setup for the Model Repository

The following information supplements the Oracle RAC Support section of these documents.

Upgrading SA to Version 9.0 in a Oracle RAC Environment



The following instructions are for a single standalone core, however, the steps are adaptable for SA Cores in a Multimaster Mesh/Oracle RAC environment.

Requirements

- The SA core must be up and running.

Pre-upgrade Tasks

- 1 Remove any installed SA patches as described in the version 9.0 *SA Upgrade Guide*.
- 2 After all patches have been removed, shutdown all SA components.
- 3 On any of the RAC nodes, shutdown the Oracle Listener, modify `listener.ora` as described in the section “Making changes to `listener.ora` on one of the RAC node server (instance)” under Oracle RAC Support in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.
- 4 Start the Oracle Listener.
- 5 Modify the `tnsnames.ora` file on the core server on which you will run the SA Installer as described in the section “Making changes to `tnsnames.ora` on SA server” under Oracle RAC Support in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.
- 6 Start the SA Management Gateway on the Infrastructure Component bundle host.
- 7 Start the Core Gateway(s) on the Slice Component bundle host(s).
- 8 Log in to SQL*Plus and grant two new privileges, create any directory and drop any directory, to the `opsware_admin` database user. These commands can be run from any RAC node:

```
❖ Sqlplus "/ as sysdba"  
❖ Sqlplus> grant create any directory to opsware_admin;  
❖ Sqlplus> grant drop any directory to opsware_admin;
```

During the Upgrade

- 1 Upgrade to SA 9.0 using the normal upgrade process as described in the version 9.0 *SA Upgrade Guide* (if necessary, fix any Prerequisite Checker errors).
 - During the interview, when prompted for the `truth.host` parameter value, specify the RAC node instance being used for upgrade.
- 2 Start the upgrade script as described in the *SA Upgrade Guide* and upgrade the Model Repository.

- 3 After the Model Repository upgrade complete, upgrade the Infrastructure Components.
- 4 After the Infrastructure Component upgrade completes, update the `vault.conf` file to use Oracle RAC's SID as described in the section “Vault.conf File Changes” under Oracle RAC Support in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.

- 5 Restart the `vaultdaemon`. Wait for all transactions to be published (use the command `tail /var/log/opsware/vault/vault.0.log` to check):

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

- 6 Ensure that the database instance is in normal mode. If the Model Repository installation was successful, then the database should be in normal mode:

```
⋄ select logins from v$instance; (logins should be ALLOWED)
```

If the Model Repository upgrade was successful but the instance is in *restricted mode*, run the following commands:

```
⋄ ALTER SYSTEM DISABLE RESTRICTED SESSION;
⋄ select logins from v$instance;
```

- 7 Restart the upgrade script.
- 8 Upgrade the Slice Component bundle host(s).

In an Oracle RAC environment, upgrade will fail when trying to start Application Deployment Manager (ADM) because it has not been configured to use RAC settings. Perform the following tasks to configure ADM:

- a Modify `/opt/opsware/da/webapps/arm/WEB-INF/classes/hibernate.cfg.xml` adding a connect string to the block that contains the "connection.driver_class" and "connection.username" entries similar to the following:

```
<session-factory>
<property name="connection.driver_class">oracle.jdbc.OracleDriver</property>
<property name="connection.username">twist</property>
<property name="connection.url">jdbc:oracle:thin:@
(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))))</property>
```

where hosts `rac1-vip` and `rac2-vip` are the RAC instances.

- b Restart ADM:

```
/etc/init.d/opsware-sas restart da
```
- c Restart the upgrade script and complete upgrading the remaining components.

Post-upgrade Tasks

After the upgrade is complete:

- 1 Update `tnsname.ora` on the SA server and `listener.ora` on the Oracle RAC instance to use the operational configuration as described in the sections “Making changes to listener.ora on one of the RAC node server (instance)” and “Making changes to tnsnames.ora on SA server” under Oracle RAC Support in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.

- 2 Restart the Oracle Listener.
- 3 Restart the SA components.

Adding a Secondary Core Using the SA 9.0 Installer in an Oracle RAC or Remote Database Environment

The following instructions assume an SA 9.0 First Core with a remote database server.

Exporting Model Repository Content

- 1 Perform a Secondary Core installation as described in the *SA Simple/Advanced Installation Guide*, Multimaster Mesh Installation chapter.
- 2 During *Phase 2: Define the New Facility*, you must set the value for the `slaveTruth.truthIP` parameter to be one of the Secondary Core's RAC nodes/instances.
- 3 Shutdown all components capable of writes on the First Core (Data Access Engine (spin), Web Services Data Access Engine (twist) and `vaultdaemon`).
- 4 A workaround is required to perform the Model Repository export remotely (due to QCR1D 113314).
 - a On the First Core's RAC instance, NFS share `/var/tmp` with the `no_root_squash` option to the SA server. Ensure that `/var/tmp/oitmp` does not already exist.



The `no_root_squash` option is required.

In the following example the SA host is on 192.168.173.214 and the RAC node is on 192.168.173.210:

```
[root@rac1pub ~]# cat /etc/exports
/var/tmp          192.168.173.214(rw,sync,no_root_squash)
[root@rac1pub ~]# exportfs -a
[root@rac1pub ~]# exportfs
/var/tmp          192.168.173.214
```

- b On the SA Model Repository (truth) host, mount the RAC instance to `/var/tmp`.


```
[root@rac1sa var]# mount 192.168.173.210:/var/tmp /var/tmp
```
- 5 Perform the export on the First Core's Model Repository (truth) host.
- 6 Copy the resulting `oiresponse.<dcNm>` and `truth_data.tar.gz` files to the Secondary Core host on which you will run the SA Installer
- 7 Set `tnsnames.ora` and the Oracle Listener to the Oracle RAC operational configuration on the SA server and RAC instance as described in the sections "Making changes to `listener.ora` on one of the RAC node server (instance)" and "Making changes to `tnsnames.ora` on SA server" under Oracle RAC Support in the *9.0 SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.
- 8 Unmount `/var/tmp` on the SA server.
- 9 Restart all components capable of writes on the First Core (Data Access Engine (spin), Web Services Data Access Engine (twist) and `vaultdaemon`).

The First Core should now be up and functioning normally.

However, System Diagnosis errors will be displayed because the Secondary Core is not installed yet, although it is now defined.

- Oracle Character Set
- Truth Garbage-Collector Parameters
- Core Gateway Configuration
- CheckSenderHealth
- CheckReceiverHealth
- Data Integrity

Adding the Secondary Core that Uses Oracle RAC or a Remote Database

Model Repository Pre-installation Tasks

- 1 Set up the Oracle RAC environment as described under “Oracle RAC Support” in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository. Ensure that the necessary UTC time and `init.ora` modifications have been made and that the required tablespaces and users have been created.
- 2 Install the Oracle full client onto the SA server on which the SA Installer is to be run.



The Oracle 11.2 client is not compatible with Oracle 11.1 databases (116363). The Oracle client version must be equal to or earlier than the Oracle server version. For an Oracle 11.1.0.7 database server, use an Oracle client version 11.1.0.7 or 10.2.0.4.

- 3 Modify the `tnsnames.ora` file on the SA server on which you will run the SA Installer and the `listener.ora` file on one of the RAC nodes as described in the sections “Making changes to `listener.ora` on one of the RAC node server (instance)” and “Making changes to `tnsnames.ora` on SA server” under Oracle RAC Support in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.
- 4 A workaround is required to perform the Model Repository import remotely (due to QCR1D 113314):
 - a On the Secondary Core's RAC instance, NFS share `/var/tmp` with the `no_root_squash` option to the SA server. Ensure that `/var/tmp/oitmp` does not already exist.



The `no_root_squash` option is required.

In the following example, the SA Secondary Core host is 192.168.173.230 and one of the Secondary Core's RAC nodes is on 192.168.173.226.

```
[root@rac3pub ~]# cat /etc/exports
/var/tmp/          192.168.173.230 (rw, sync, no_root_squash)
[root@rac3pub ~]# exportfs -a
[root@rac3pub ~]# exportfs
/var/tmp          192.168.173.230
```

- b On the SA Model Repository (truth) server, mount the RAC instance to `/var/tmp`.

```
[root@rac2sa var]# mount 192.168.173.226:/var/tmp /var/tmp
```

- 5 Install the Secondary Core's Model Repository as described in the *SA Simple/Advanced Installation Guide*. Run the SA Installer using the `oiresponse.<dcNm>` response file you created and copied in [step 6](#) on page 138.
 - `truth.host`: verify this is the RAC instance IP address.
 - `truth.orahome`: ensure this is the path where the Oracle full client is installed.

After Model Repository Installation

- 1 After the Model Repository (`truth`) is installed, unmount `/var/tmp` from the SA server.
- 2 Install the Infrastructure Components.
- 3 After the Infrastructure Components installation completes, modify the `vault.conf` file to use Oracle RAC's SID as described in the section "Vault.conf File Changes" under Oracle RAC Support in the 9.0 *SA Simple/Advanced Installation Guide*, Appendix A, Oracle Setup for the Model Repository.

- 4 Restart the `vaultdaemon`. Wait for all transactions to be published (use the command `tail /var/log/opsware/vault/vault.0.log` to check):

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

- 5 Install the Slice Components.

In an Oracle RAC environment, install will fail when trying to start Application Deployment Manager (ADM) because it has not been configured to use RAC settings. Perform the following tasks to configure ADM:

- a Modify `/opt/opsware/da/webapps/arm/WEB-INF/classes/hibernate.cfg.xml` adding a connect string to the block that contains the "connection.driver_class" and "connection.username" entries similar to the following:

```
<session-factory>
<property name="connection.driver_class">oracle.jdbc.OracleDriver</property>
<property name="connection.username">twist</property>
<property name="connection.url">jdbc:oracle:thin:@
(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)))</property>
```

where hosts `rac1-vip` and `rac2-vip` are the RAC instances.

- b Restart the installation and complete installing the rest of the components.

After Installation is Complete

- 1 After installation completes, modify the `listener.ora` and `tnsnames.ora` files on both the SA and RAC instances to use the RAC operational files.
- 2 Restart the Oracle Listener.
- 3 Restart the SA components.

Storage Visibility and Automation User Guide

The following new default values apply to Chapter 2, Asset Discovery:

```
com.creeppath.agent.common.devices.scheduled.full.sync.max.wait.minutes=10080  
com.creeppath.agent.common.devices.full.data.collection.minutes=720  
com.creeppath.agent.common.devices.manual.full.sync.max.wait.minutes=10080
```

Storage Visibility and Automation Installation & Administration Guide

The following new default values apply to Chapter 5, SE Connector:

```
com.creeppath.agent.common.devices.scheduled.full.sync.max.wait.minutes=10080  
com.creeppath.agent.common.devices.manual.full.sync.max.wait.minutes=10080  
com.creeppath.agent.common.devices.full.data.collection.minutes=720
```

