Server Automation

Software Version: 10.50

Release Notes

Document Release Date: July 2016
Software Release Date: July 2016

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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 Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

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: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

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

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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 HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPESW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/.

Contents

Introduction

This document provides an overview of the Server Automation 10.50 release. It contains important information not included in the manuals or in the online help.

Up-to-date documentation

All the documentation is available from the new SA 10.50 Documentation Library. See the Documentation Information section for instructions on how to use the Documentation Library to access the guides and white papers relevant to this release.

For the most updated release notes, see the SA 10.50 Release Notes on the HPE Software Support website.

Support and compatibility information

For complete SA support and compatibility information for this release, see the SA 10.50 Support and Compatibility Matrix.

For more information about supported configurations, see **Customer installable SA Core configurations** in the SA 10.50 Planning Guide.

Audience

This release notes contains information pertaining to the installation and maintenance of Server Automation, Application Deployment Manager, and DMA integration.

New in this release

This section describes new functionality and other release-specific information.

Windows operating systems supported on the SA Client

This section lists the operating systems supported on the SA Client.

- Windows Server 2008 R2
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2012
- Windows Server 2012, R2

New Linux Service operating system

The new Linux Service OSs provided with SA 10.50 is based on CentOS.

Service OS (SOS) bits are not available for the PPC and IA processor architectures in the current distribution.

In case of an upgrade, the existing RHEL IA and PPC Service OS bits will not be removed. The existing RHEL x86/x64 bits will be renamed, adding 'rpmsave' to the original name. If you want to reuse these bits, restoration can be performed by replacing the linux50/linux60/linux60x64 folder with rhel50rpmsave/rhel60rpmsave/rhel60x64rpmsave, at this path: /opt/opsware/boot/tftpboot/ and /opt/opsware/boot/kickstart/. If you are performing a new installation, there will be no Linux Service OS for these two processor architectures.

SE Linux support in SA

SE Linux is supported in Permissive or Enforcing modes for RHEL 6.6. For more details, see SA 10.50 Administration Guide.

New for SA Web Client

The SA Web Client is now only used for downloading the SA Client launcher. The Web Client can be accessed as before, by navigating to a slice IP address or hostname and it features a completely re-designed home page that contains a Download Server Automation Launcher button, information about SA version and build and a link to the HPE Support site.

The functionalities that were previously available in SA Web Client can now be accessed from the SA Client as follows:

- Service Levels can now be found in the SA Client under **Administration** > **System Configuration**. For more information on SA Service Levels, see the SA 10.50 Administration Guide.
- OS Installation Profiles are now created through a script on an SA Core. For more information on OS Installation Profiles, see **SA Provisioning** in the SA 10.50 Administration Guide.

New for SA Agent

Configured debugging

Now you can configure debugging for ptymonitor through the ptymonitor.debug_name parameter in the agent's configuration file, agent.args.

Disabled RC4

In this release, RC4 has been disabled for SSL encryption.

Importing users

The new custom attribute **hpsa_preserve_solaris_user_home_path** allows you to import users using your user-home path in **/home/…**. In previous SA versions, the import tool added **/export** to the path.

To exclude the **/export** addition to the path, set the custom attribute to managed server.

Changes made to the Agents installed on a non-system drive

For agents installed on a non-system drive (a feature available from SA 10.21 for Windows platforms), the agent uninstaller removes symbolic links on the system drive and all agent files, except the target directory.

Selecting PAPXs after Agent installation

Using ADT (Agent Deployment Tool) you can select a maximum of 10 PAPXs to be run sequentially after the agent is successfully installed. If one of the APX scripts fails, the system stops at that step, and does not run the remaining APXs, and reports the job as FAILED.

> **Note:** In case of an error during the APX script run, the system will not roll back the currently or previously successfully run APXs.

This release includes three PAPXs for the following functionality:

- Assign Server to Customer
- Attach Server to Device Group
- Attach Server to Software Policies

New for SA Client launcher

Authentication to the SA Core is now done in the SA Client, after the Launcher has downloaded the required files. The SA Client Launcher now accepts only one input from the user: the SA Core hostname/IP address. A new window appears, where you need to enter the SA username and password. For more information, see **Server Automation** in SA 10.50 User Guide.

Java Web Start has been removed from the SA Client Launcher. The functional changes that resulted are as follows:

- Log files are now located at the path **<HPE_Server_Automation_Home>\logs**
- The **Show Java Console** option is no longer available and is assumed checked when connecting to SA releases prior to 10.50
- SA Client application data is reused when connecting to core servers with the same build number

Security and Third-Party upgrades

TLS Compliance

According to PCI DSS v3.1 standard, any cryptographic protocol lower than TLSv1.1 is considered weak. Starting with 10.50 release, SA allows protocol selection (possible values: TLSv1, TLSv1.1, TLSv1.2). For more details, see SA 10.50 Administration Guide or SA 10.50 Upgrade Guide.

New upgraded Third-Party product

Python upgraded from Python 2.7.3 to Python 2.7.10.

JBoss migration

From SA 10.50, the Application Server used by the Web Services Data Access Engine (Twist) component migrates from Weblogic to Wildfly (formerly known as JBoss). See "Deprecation and end-of-support announcements" on page 15 for details on what is affected by this migration.

New for audit and compliance

A new optional element, preserveExceptions, is available in Audit Policy Filters. The element can be set to **Yes** or **No**.

New for certificates

Added CRL (Certificate Revocation List) support for access to SA using SA client with smart card authentication.

New for localization

SA 10.50 will be localized to Simplified Chinese, Japanese, German, Russian, French, and Spanish.

New for OO-SA integration

Updates pertaining specifically to the OO-SA integration (Server Automation operations performed within Operations Orchestration) are delivered via the HPE Live Network.

New for Oracle database and model repository

For changes to the Oracle Database and Model Repository, see **Oracle setup for the model repository** in SA 10.50 Installation Guide.

New for patching

Red Hat dynamic patching

SA 10.50 adds support for Red Hat dynamic patching. Dynamic patch policies do not contain a list of policy items like their static counterpart, but apply the required updates to the managed servers based on the vendor recommendations. Dynamic patching offers better performance and scalability over static patching through software policies and it is the recommended way to keep your managed servers up-to-date. For more details, see **Patch management for Red Hat Linux Enterprise** in SA 10.50 User Guide.

SA SUSE Manager Importer

SA now offers a SUSE Manager Importer tool based on the SA RedHat Importer. The tool is capable of importing packages and errata from the SUSE Manager 2.1 Server and creating SA Software Policies for errata and packages hosted by SUSE Manager. For more information, see White Paper: SUSE Manager SLES Importer and the SA 10.50 Support and Compatibility Matrix.

Important: See Deprecation and End-of-Support Announcements for important SA Agent version deprecations and end-of-support announcements.

Red Hat Satellite 6.x support

Modifications have been made to the HPE SA Red Hat Network (RHN) import tool to support content download from Red Hat content delivery network (CDN) using Red Hat subscription management (RHSM). This allows you to download content for Red Hat Enterprise Linux 7 (RHEL). For more information on how to set up and use the HPE SA Red Hat importer tool, see Using the Server Automation Red Hat Importer.

New for OS provisioning

New features:

- New Run OS Build Plan UI.
- Support for deploying platforms on UEFI with secure boot enabled on HPE ProLiant.
  - New Linux 7 service OS with network and CD boot support for Legacy BIOS, UEFI and UEFI with secure boot.
  - New WinPE4 service OS with network and CD boot support for Legacy BIOS, UEFI and UEFI with secure boot.
- Improved customer assignment:
  - The "Assign Customer" step is now part of the OOTB build plans.
  - The UI is modified to be able to assign the server to a customer.
- New UAPI to allow the creation of customized pre-unprovisioned servers. See ServerService.create (ServerVO vo, ServerHardwareVO hwVO).
- Content SDK to help customers with the development and deployment of Build Plans. For more details see the documentation under /Opsware/Tools/Content SDK/ContentSDK-<version>.zip.

Updates:

- ProLiant content upgraded to Insight Control Server Provisioning 7.5.1.
- WinPE 3 and 4 based service OS drivers updated.

New platforms supported by build plans:

- Solaris 10 SPARC
- Solaris 11 SPARC
- Windows 10

- SLES 12
- Ubuntu 14.04
- Novel OES 11

For more details on the newly supported platforms see **Addendum Provisioning Feature** in the SA 10.50 Support and Compatibility Matrix.

For all platforms, OS Sequences are deprecated in SA 10.50 and later. The migration of any existing OS sequences to OS Build Plans for these platforms is strongly recommended.

For more details about the new features see **SA provisioning** in the SA 10.50 Administration guide.

New for software management

RPM Rollback

SA 10.50 introduces RPM rollback functionality based on yum history, available for yum versions 3.2.25 or later. In previous releases the RPM rollback functionality was only available on Linux servers where the installation was done using RPM versions 4.2 to 4.6, but the upstream feature was discontinued. For more details see **Software Management** in the SA 10.50 User Guide.

Unit history

Starting with SA 10.50, all changes made to the units in the SA Library can be tracked using the new History element. The logged information includes name, description, platforms, location, install path, scripts, and flags.

Timeout handling for remediation and installation jobs

Server Automation now offers improved timeout handling for remediation and installation jobs. After a timeout occurs and until the job execution stops, the status of the server is changed to Stopping. While in the Stopping state, the agent does not take on any additional jobs and completes any job that is currently in progress. Moreover, if the timeout occurs during an agent reboot, then after restarting, the agent will not resume the job. After the job execution stops, the server will be marked as Timed Out.

This fixes the discrepancy of the core showing the job as Failed because of a timeout, while the agent is performing the job.

Job enhancements

Software remediation jobs now support a secondary expansion mode (“At runtime”) for device groups, software policies, and patch policies. This way, when a remediation job is scheduled to run in the

future, the device groups, software policies, or patch policies are expanded when the job is started, compared to previous releases where the expansion was done at the time the job was created.

SPARC provisioning

SPARC servers can be provisioned now using OS Build Plans and not just OS Sequences. However, both the methods cannot be used at the same time. The default configuration is the OS Build Plans provisioning mode.

To ease the switch between modes and the dhcpd.conf configuration, use the following script:

```
/opt/opsware/boot/jumpstart-sparc-ogfs/tools/switch_OSS-OSBP.sh
```

When run, it will print the current provisioning mode for SPARC servers and request for your confirmation before switching the mode. If you continue, the script will backup the dhcpd.conf file, perform the required changes and restart the dhcpd service.

Security features

SA Client Session Inactivity is enabled and set by default to 30 minutes. This will lock the SA Java Client if you are idle for the specified period. You need to re-enter the password to unlock the SA Java Client. This setting will not be enforced when upgrading installations that have any custom settings applied under **Administration** > **Users and Groups** > **Security Settings** > **Password Policy Settings**.

RHEL7 Core Platform

SA can be installed on servers that are running Red Hat Enterprise Linux 7 (x86_64).

> **Note:** On RHEL 7.2, you must upgrade systemd package at least to version 219-19.el7_2.4. Otherwise, the core services will not start automatically upon reboot. See errata https://rhn.redhat.com/errata/RHBA-2016-0199.html for more details.

SA failover and High Availability

The SA 10.50 Administration Guide provides information on how to achieve failover, server load balancing, and high availability in the SA environment.

SA backup and restore best practices

The SA Backup and Restore Best Practices white paper provides the best practices you can use to backup and restore SA with minimal data loss in a situation where SA has been adversely affected by data or power failures.

New version of HPE Live Network Connector

The Live Network Connector (LNc) that is installed on the SA core at: /opt/opsware/hpln/lnc/bin is outdated and can no longer be used to download content.

You need to download the latest version of LNc and install it on the core.

1. From HPELN, download the latest version of the HPE Live Network Connector.
2. Copy the new version to the SA core at /opt/opsware/hpln/lnc and install it: #./install

After installation is successful, LNc should work correctly.

Deprecation and end-of-support announcements

This section lists deprecated platforms, features, and agents for this release as well as previously deprecated items that have now reached the end of their support lifecycle.

Deprecations

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

Deprecated products or platforms

Managed platforms

The following platforms are deprecated in SA 10.50:

- Windows Server 2003
- Windows Server 2003 R2
- Windows XP

Deprecated components

SA Agent deprecation and upgrade requirement

SA 10.50 no longer supports SA Agents associated with SA 9.10 or earlier versions. Therefore, at a minimum, any SA Agents with version 9.10 or earlier must be upgraded to an SA Agent that is version 9.11 or later.

See the SA 10.50 Upgrade Guide for instructions on upgrading your SA Agents.

Application deployment

The Application Deployment feature is deprecated in SA 10.50 and it is disabled by default.

RHN import

The rhn_import binary has been deprecated in SA 10.50.

You can now download and import content into the SA Library using the new redhat_import binary which supports downloading content from legacy RHN portal as well as from Red Hat content delivery network (CDN) using Red Hat subscription management (RHSM). This allows you to also download

content for Red Hat Enterprise Linux 7 (RHEL). For more information on how to set up and use the HPE SA Red Hat importer tool, see Using the Server Automation Red Hat Importer.

Deprecated API methods

The following API methods were removed following the move of application configurations into folder in SA 10.50:

- com.opsware.acm.CMLVO#setCustomers
- com.opsware.acm.CMLVO#getCustomers
- com.opsware.acm.ConfigurationVO#setCustomers
- com.opsware.acm.ConfigurationVO#getCustomers
- com.opsware.acm.Configurable#update
- com.opsware.acm.ConfigurationService# attachToConfigurable

OS provisioning OS Sequences

OS Sequences were replaced with OS Build Plans. For details and instructions, see **SA Provisioning** in SA 10.50 Administration Guide.

Embedded reports

The Embedded Reports feature is deprecated in SA 10.50.

Unsupported

Unsupported platforms

The following platforms are no longer supported in SA 10.50:

- AIX 5.3
- Oracle Enterprise Linux 4
- Red Hat Enterprise Linux AS 3, AS 4, ES 3, ES 4, WS 3, WS 4
- SuSE Linux Enterprise Server 9
- SunOS 5.8, 5.9
- Windows Server 2000

- VMware ESX 3, 3.5
- VMware ESXi 3, 3.5
- VMware ESX 4.0
- VMware ESX 4.1
- VMware ESXi 4.0
- VMware ESXi 4.1

JAVA RMI clients

Java RMI Clients (built previous to SA 10.50) will not be able to connect to SA 10.50 cores. To fix the issue you need to use the latest opswclient.jar (from SA 10.5x) and run the RMI client with Java 8. Note that opswclient.jar in SA 10.50 is not backward compatible, that is, you cannot use it to connect to an SA 10.2x (or older) core.

Unsupported products

AI reporting

AI is announced End-Of-Life. It has been replaced by Operations Bridge Reporter (OBR).

SE connector

The SE Connector is removed in SA 10.50.

Host storage extensions

The Host Storage Extensions component is removed in SA 10.50.

Database scanner

The Database scanner for Oracle component is removed in SA 10.50.

Unsupported features

Application server

From SA 10.50, the Application Server used by the Web Services Data Access Engine (Twist) component migrates from Weblogic to Wildfly (JBoss). Hence, any PSO customizations that are Weblogic specific will be lost in case of an upgrade. Standard customizations (example: memory settings, logging levels) in twist_custom.conf are preserved.

Agent upgrade tool

The Agent Upgrade Tool that is run from the OPSH shell and allows upgrading the agents on managed servers is no longer supported. As of SA 10.0, a replacement APX was introduced that has several improvements and can be run from the SA Client.

Installation

New for installation

- Install/Upgrade SA 10.50 as users with root capabilities
- Changes made when adding a new core

Changes made when adding a new core

Adding a new (secondary) core to a mesh is performed in two stages, as before:

1. Defining a new facility and exporting required data (by running the hpsa_add_dc_to_mesh.sh script)
2. Installing the new secondary core (by running the hpsa_install.sh script)

The following changes were done in the process of adding a new core:

- The possibility to define and install the new core without providing credentials to the remote database servers (for the primary or secondary cores).
- The tar.gz file resulting after defining the new facility (ie. running the add_dc_to_mesh script) has been split. The database export and the CDF for the new core are no longer included. This provides the possibility to copy the database export directly to the secondary core database server and the tar.gz file and the CDF to the machine where the secondary core install will be performed.
- Two modes for transferring the files to the secondary core have been defined as follows:
    - manual: files are exported but not transferred to the secondary core. SSH credentials for the remote database servers are NOT required.

  - automatic: files are transferred to the secondary core. SSH credentials for the Oracle (primary and secondary) servers are required.

- When performing the secondary core installation, no commands will be run on the database server if it is not the SA-supplied one. In such a case users must ensure that prerequisites are met, as displayed by the on-screen instructions.

  For details, see the SA 10.50 Installation Guide.

Users supported by the SA installer

The following new users are supported with the SA installer:

User Name	Machine Type	Description
root user	Local	A root user
regular user	Local	A regular user who has permissions to invoke commands as root with sudo capabilities. Note: When you use a regular user for performing the installation or rollback of a core patch, make sure you invoke the command using sudo. For example: sudo <distro>/ opsware_installer/hpsa_install.sh
root user	Remote	A root user, including root ssh access
regular user	Remote	A regular user with sudo capabilities (including user ssh access) WARNING: Password-less sudo is not supported for regular users with sudo capabilities.

For details, see the SA 10.50 Installation Guide or SA 10.50 Upgrade Guide.

Renaming SA default folders

WARNING: Do not rename SA default folders, including the Package Repository folder.

New optional parameters for the enable_ipv6.sh script

There are two new optional parameters for the enable_ipv6.sh script:

- -i <IPV6 address>: use specified IPV6 address instead of autodiscovered based on hostname DNS AAAA resolution.
- -n : do not start/restart SA components when making configuration file changes.

Known issues

This section describes known issues for SA. The tables list issues first alphabetically by Subsystem, then numerically within each subsystem.

QCCR1D	Symptom/Description	Platform	Workaround
AGENT			
192728	When using the ADT Scan feature, an error message appears in the SA Client when scanning ranges using * or /24 (CIDR) notations.	Independent	An nmap (the tool used to make the network map) error will be displayed, but it does not have any negative impact on the scan itself. It is an issue with nmap (bug raised on nmap).
193587	In some scenarios and network topologies, when scanning for an IPv6 enabled server the SSH port it is shown as unavailable and the agent cannot be deployed.	Independent	From the SA Client, modify the ADT scanning parameters based on the network topology, proy and firewall rules.
224743	HP-UX v11.11 Agent does not start correctly after reboot.	Independent	From SA 10.10, agents use OpenSSL 1.0.1h, which require the presence of "KRNG11i - HP-UX 11.11 Strong Random Number Generator" package on the HP-UX 11.11 Operating System:

			https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=OPENSSL11I To ensure that the SA Agent is communicating correctly with the core, you must install the "KRNG11i - HP-UX 11.11 Strong Random Number Generator" package for HP-UX 11.11: https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=KRNG11I
APX CONTENT			
111925	A deployment which includes a Configuration File component fails without any warning or error when attempting to place a file in a directory which has not been created in advance.	Independent	Ensure that a code (or other type of ADM component) creates the destination directory in preparation for placement by the Configuration File component.
AUDIT AND COMPLIANCE			
151552	If you cancel a running audit job, and a target server shows a "SKIPPED" job status in the audit results, until an audit has successfully run, the server's compliance view shows the following incorrect status for the policy: “Policy has changed since the last scan”.	Independent	Rerun the Audit.
183967	Running a "Users and Group" remediation job with multiple uses and user groups will fail with error message: "No Group found".	Independent	Run a "Users and Group" remediation job with user groups followed by a remediation job to remediate users that belong to the remediated user group.
CERTIFICATE			

184908	Occasionally, core recert status will show core recert session not in progress, even though core recert has been executed. May be most applicable to FIPS-enabled customers.	Linux	Generally waiting 10 minutes or so seems to resolve the problem.
189893	After core recert infrastructure-only (non-slice) boxes will not have the proper certificates for the word_upload component and work_ upload may not work properly on that box.	Linux	May be resolved manually by copying certificates in /var/opt/opsware/crypto/word_uploads on box with slice to the corresponding directory on the infrastructure-only box.
191875	During core recert the security.conf file (in the directory /etc/opt/opsware/crypto) is created or updated on all cores, slices and satellites. The core recert process has no obvious way to reach an oracle-only box that is part of the mesh, so the file is not propagated.	Linux	Customers should not experience any problems because of this. If desired, a copy of security.conf can be copied from one of the mesh's cores to the oracle-only box.
225032	There are chances for phase 1 and /or phase 7 to fail in single core or multimaster mesh installations that have satellites. This is because the core recertification tool is unable to determine if certain files exist on satellites. This is a temporary condition that can occur after the Gateways restart in these phases.	Independent	Rerun the phase that fails, using the --doit flag to allow it to complete successfully.

GATEWAY			
193091	After upgrading core from 10.0 to 10.20 and up, the 10.0 satellite is unreachable.	Independent	See https://softwaresupport.hpe.com/group/softwaresupport/searchresult//facetsearch/document/KM01365141
HPUX-VIRTUALIZATION			
157368/160408	Search with IP Address or Hostnames on Add Virtual Server screen does not list HP-UX machines.	HP-UX	Servers can still be listed when "All" is selected on the Add Virtual Server screen.
MANAGED PLATFORMS			
191478	CentOS 7 Build Plan fails with TypeError after migration from SA 10.02 with platform installed to SA 10.2.	Independent	None.
227335	After rebooting an SA machine with RHEL 7.2, SA core services do not start.	Independent	Upgrade systemd RPM to at least systemd-219-19.el7_2.4.
OCC			
135460	Not able to select servers in Run Custom Extensions submenus.	Independent	None.
172654	Unable to start httpsProxy. SA installer should validate /etc/hosts against multiple 'localhost' definitions.	Linux	In the /etc/hosts file, remove 'localhost' and 'localhost.localdomain' from the definition line that begins with:1. Save the file, and retry the installer. Note: This installer issue is only valid for Major release not CORD release.
191941/192463	The SA Client progress bars are reduced at a line and doesn't indicate progress for Windows 8/8.1/2012/2012 R2.	Independent	None.
213050	Launcher cannot log in to SA Core using its IPv6 address.	Independent	This is a Java Web Start issue, not an SA issue. No workaround.

OS PROVISIONING			
114523	OS Sequences can fail with persistence error when sequence includes a device group and is run repeatedly	Independent	Use Build Plans to implement the equivalent use-case.
175069/213698	Cannot use an OS Build Plan to provision Windows Server 2012 to a UEFI ProLiant server's second hard disk unless both of the server's hard disks are empty.	Windows 2012	Ensure that all data has been removed from both hard disks then retry the provisioning.
213391	Running default BP "Add Migrated Linux Server" fails at "Set One Time PXE Boot"	Independent	These build plans are specific to RDP to ICsp migration, so are not applicable to SA. This issue is caused by incorrect usage of the product.
PATCH MANAGEMENT			
100566	When the last patch in job has reboot-normal setting, the job status shows incorrect "Reboot later" information for this patch. Although the reboot is performed correctly, when previewing remediating a patch policy on a server, or view the job status for a patch policy that is already remediated, the reboot setting might incorrectly display "Install and Reboot Later" when it should display "Install and Reboot".	Solaris	A workaround is not required because the reboot is performed correctly, even though the display may be incorrect.
102713	Number of Rules of patch policy	Independent	From an overall compliance perspective, SA is reporting the correct

	compliance is not correct after remediation or installation of patches.		color. It just doesn't report the same number of patches before and after the scan. This is controlled by how Microsoft reports applicable/installed patches.
146902/157891	Solaris 11 Patch policies must prevent the user from changing the reboot option from the default option 'hold all server reboots until all actions are complete'.	Solaris	Always ensure that the reboot option is 'Hold all server reboots until all actions are complete' when remediating Solaris 11 Patch Policies.
148400	After MBSA import completes, it takes a long time to update patches in library and database info in admin page	Windows	No workaround required as it does not impact the functionality.
151092	Customers see duplicates between HPELN Patches and WSUSSCN2.CAB Patches. They have to run scripts that delete one of the conflicting patches from the SA database.	Independent	Version agnostic scripts have been provided in a hotfix which can be used to remove patches from the SA database. https://patch-central.corp.hp.com/crypt-web/protected/viewContent.do?patchId=QCCR1D151092
161961	The windows 2008 R2 SP1 consists of 2 binaries. When the user selects binary with file name windows6.1-KB976932-X64.exe and clicks uninstall in actuality the file gets uninstall and the server reboots and is now on Windows 2008 R2 RTM but the job times out and fails.	Windows 2008 R2	No workaround. Problem corrects itself with next scan.
162337	Windows 2k12 software policy remediation fails with the following type of	Windows 2012;Windows 2012 R2	Import and run the latest (later than October 2012) Microsoft patch CAB file once. You should only have to do this one time.

	error: 'AGENT_ ERROR_PATCH_ DATABASE_ CERTIFICATE_ ERROR'.		
SAV (SERVER AUTOMATION VISUALIZER)			
181473	SAV does not show IPv6 inet addresses or IP address for loopback.	Independent	IP addresses may not appear in IPV6 format for SAV Isaac release.
SEARCH			
92244	Searching on extended ASCII (words contains the "ß") characters returns no matching results.	Independent	No workaround till extended ASCII characters are supported.
SERVER			
156389	Users and Groups SMO will not report all the groups that are created on a Windows 2012 Essentials. If user properties are edited, these changes will not be reported by the SMO. This means that audits with U&G rules will not be relevant on a Windows 2012 Essentials.	Windows 2012	None.
192013	Windows Local Security Settings SMO reports incorrect Security Settings for Not Applicable entries.	Independent	None.
193063	SMTool upload fails when /var/tmp folder is not present on the twist box where the command is run.	Independent	Create the expected directory structure.
SOFTWARE MANAGEMENT			

159841	When performing a core upgrade, you might experience conflicts originating from the UNITS and REALM_ UNITS tables.	Independent	In order to continue with the upgrade process, the user needs to either manually resolve the conflicts or to clear them using the force resolver script.
163518	"End Job" button is still enabled after the job has completed.	Independent	None.
179479/179480	Recurring app config compliance jobs uses tokens with a one year lifetime.	Independent	None.
SPIN (DATA ACCESS ENGINE)			
193285	All gateways in a satellite facility should have the same weights defined for primary and backup tunnels.	Independent	None.
TRUTH (MODEL REPOSITORY)			
166334/188553	SA installed Oracle RDBMS modifies file /etc/sysconfig/selinux and inserts entry for SELINUX regardless of whether a previous entry exists.	Linux	If multiple entries exists then keep the entry that is created by SA. Oracle (SQL*plus, OCI etc.) will not function properly if SELINUX is set to 'enforcing'. It is suggested that SELINUX be set to 'disabled' or 'permissive'.
191511	There is a connectivity issue from MM infra slice to the secondary core DB when secondary core's database is in a RAC configuration and that secondary RAC fails over to a second node. Currently, a manual change to the MGW properties file and the tnsnames.ora files are needed to achieve a failover.	Independent	Bypass the gateway connection from the primary core to the secondary and communicate to the RAC. This will provide the ability to continue to communicate if one node goes down. Also, even if the one RAC node goes down, no data is lost it is that communication needs to be established to the RAC (manual process) and the Muli-master will sync the data.

UCMDB			
194366	The data from SA is not loaded correctly and completely when UCMDB server is configured in multi-tenancy mode.	Independent	None.
VIRTUALIZATION			
141907	If you configured the number of cores per socket using the native vSphere client, and modify the number of virtual processors with a Modify VM job in SA, the CPUs might end up in an invalid configuration. When you edit the CPU settings in the native vSphere client, this error, “Number of cores per socket cannot be greater than number of virtual CPUs” occurs when the configuration is invalid.	VMware	If the number of cores per socket for a VM is greater than 1, and you want to modify the CPUs: From SA, set the number of Virtual Processors as a strong multiple of the number of cores per socket. Or, use the native vSphere client to modify the CPUs.
160891	If a Create VM, Clone VM, or Deploy VM from VM Template job fails running the OSBP, and the VM ends up in Build Server Failed state, the VM cannot be deleted from SA Client.	Independent	Delete the VM from native vendor tool and reload in SA.
183608	The Openstack VM server is reachable externally only through its public floating IP, not through its internal private IP. The SA Agent is installed on the server using its floating IP, so	Independent	Do not try to change the IP from its “Default” setting to the internal OpenStack IP.

	eventually the management IP of the server is set to its floating IP. The server's operating system is not aware of the floating IP, so the SA Agent is unable to gather this information. As a result, the server's floating IP is not present in the interface list for this server nor in the Management IP drop-down list on the server's Network view.		
WORKLOAD MANAGER			
166350	Jobs remain with a status of Active, even though their associated tasks show a status of Success.	Independent	This issue occurs only in multi-core mesh installations where the SA Jobs are being approved using Operations Orchestration on all the cores of the mesh. To work around this issue, setup OO workflow only on the primary core of the mesh.
INFRASTRUCTURE-CORE			
184455	Running Core Recert procedures on a FIPS-enabled core will cause the buildmgr core component to fail to start after Phase 9.	Independent	To resolve this issue: 1. Make sure for all the core boxes and all the satellites boxes in the mesh, /etc/opt/opsware/crypto/security.conf has the FIPS field set to 0. 2. Start the Core component in the order specified by Core Recert document.
226639	When prerequisite checks are run on a 10.5 core (example: when adding a slice to an existing core), the following message may appear for the servers that have slice installed: "FAILURE Cannot find installation	Independent	In such a case (the server for which the message is displayed has only the Slice Component bundle installed), it is safe to ignore this message.

	SQLPlus".		
227335	If you reboot a machine with RHEL 7.2 SA, services do not start after reboot.	Independent	On RHEL 7.2 you must upgrade systemd package to at least version 219-19.el7_2.4. Otherwise the core services will not start automatically upon reboot.
INTEGRATION			
212406	After upgrading a core from IMR1 to IMR5, the SA-OO FLow Integration is not working.	OO Integration	Any SSL certificates added to the previous JDK will also need to be re-added to the new JDK(cacerts) file.
DCML EXCHANGE TOOL (DET)			
142522	DET hangs during the CBT export operation and the process is not completed.	Independent	Run with a single CBT thread by setting cbt.numthreads=1 in the CBT configuration file. The default location on the SA core for the configuration file is: /opt/opsware/cbt/cfg/default.properties.

Fixed issues

The Fixed Issues table includes issues that:

- Were found during SA 10.50 release period.
- Were in the Known Issues table, but are now fixed.

The table lists issues first by subsystem, then numerically within each subsystem.

Feature Area/QCCR1D	Symptom/Description	Platform
AGENT		
210057	Agents can no longer communicate with the core due to SSLError: disabled for fips.	
210440	package.dbg is increasing in size uncontrollably.	HP-UX
132960	Last Logoff Time is not set when users log out of Windows.	Windows
191459 C	Presence of libeay32.dll interferes with agent functionality.	Windows

191450 C	All future peval commands fail because of corrupt persisto file.	
194086 C	Windows watchdog value should be parameterized.	Windows
193224 C	Run communication test fails when more than 100 servers are selected (reachable and unreachable).	
194543 C	shadowbot does not make a reverse DNS call to log the hostname of the client.	Linux
201693 C	ADT becomes root and does not properly set the sudo algorithm.	Linux
205450 C	Agent startup fails on Windows Domain Controllers.	Windows
210421 C	During software registration on a Solaris managed server, the following error message appears: **unable to extract installed package list: 32512**.	Solaris
210428	Agent installation takes a long time when /etc/hosts has many lines.	
213522 C	Spoke spawned sub processes does not terminate on timeout.	Linux
214282 C	During hardware registration, the device UUID is set to "None".	Windows
215121 C	OGFS uapi method invocation ignores false boolean value.	AIX
216891 C	The shadowbot can return invalid characters in the HTTP status line for error responses.	Linux
218438 C	Error messages **MaxMessageSizeExceededException** appear repeatedly in hub.log.	Linux
224326	shell_rdp_handler.py should connect only to RDP-speaking Terminal Services.	Linux
AUDIT AND REMEDIATION		
193457 C	"Remediate all" preparation takes a long time on audits with many devices.	Linux
194053 C	Exceptions are deleted from the Audit when promote changes on the Audit Policy.	Linux
	'Remediate All' preparation takes a long time for audit with a large number of non-compliant target servers.	Linux
APX		
162834 C	OS BP fails and displays the error message: **Failed to inject required settings.[Errno 2] No such file or directory: '/tmp/osbp_info/media_server'**.	
187113 C	'BRDC SA agent sanitizer' APX blocks VMware customization	

	specs.	
209759	"Change user passwords for selected servers" fails to change the password when the UNIX server has a locale with chars set outside the ASCII.	Linux
BUILD		
191698	zip231 binary in agent hotfix causes various agent failures.	
CPE		
192139 C	Running script against a device group containing a server managed by v12n and a deactivated agent fails.	
193042	Installer does not calculate correctly the necessary free disk space for DB export when adding a new core to a Mesh.	Linux
193649 C	Agent does not work properly when code page cp28605 is set on managed Windows platform.	
193663 C	rhn_import fails with the error "httperror_seek_wrapper: HTTP Error 403: Forbidden".	
194419 C	Agent init.d script fails to run on AIX when /etc/environment contains a variable declaration that already exists and is read-only.	AIX
194406 C	ptymonitor crash issue occurs when running /opt/opsware/agent/pylibs/cog/bs_software due to missing PATH env var.	Linux
202175 C	Failed to take registry snapshot on Chinese Windows. UnicodeEncodeError: 'cp950'	Linux
215471 C	Permission Denied error appears when running audits against servers that are attached to customers imported with cbt.	Linux
215547 C	opswgw.HijackService is broken because of IPv6 support.	Linux
215606 C	NGUI Job Logs: Failed jobs are listed when Status = "succeeded" is selected.	
218522 C	Waybot command proxy failover is broken for all versions of SA that use python 2.7.	Linux
218594 C	Spinclient masks OPLET response is returned if it is not an XMLRPC response.	Linux
224581 C	SLES remediation with Zypper may choose an older kernel to install.	Linux
DEPLOYABILITY		
206362	Catch-all exception handler in update_sw_policy.py obscures	

	deeper exceptions.	
189986	hpsa_add_dc_to_mesh.sh is not working correctly with a remote DB running on Solaris 10 server.	Linux
192413 C	How to keep SSL from using particular ciphers Port: 5678 HPESA vaultdaemon.	
190859 C	Giving custom realm_name to a sat [different from facility name] breaks the functionality.	
183786 C	Tnsnames.ora should not be created/changed on the remote DB.	Linux
190924 C	SA upgrade to SA 10.10 fails with database connection error for opsware_admin user.	Linux
191024 C	Documentation states that libxml2-python must be removed during install.	
194905	Installer fails when there are two dmp files to import.	Linux
201846	Adding a separate slice asks for truth dump archive when it should not.	Linux
204765	NGOI: InstallSAS state dpdump directory search/check never fails.	
205370	Upgrade process fails when smb service is disabled in startup script.	
110791 C	Feature to delete a facility in SA.	
215597	Installer does not perform DB prereq checks when it warns user that their DB version is not supported.	
INFRASTRUCTURE-CORE		
208105 C	Spin software registration logging is too verbose, causes performance bottleneck.	
195146	When connecting to one server, followed by a second, the authentication performed on the second connect uses the authentication from the previous connection.	
194985 C	SA OpenSSL vulnerability - CVE-2014-3571.	Linux
209890 C	spin:1004 load balancing rule should be not be set to STICKY.	
221170	There is reip.sh functionality difference between 9.x & 10.x. Cannot rename without changing IP.	Linux
203725 C	RSA <SecurIDAuthenticator> unable to load ./libsecuridwrapper.so.	
JBOSS MIGRATION		

192921	SA upgrade process fails intermittently with ArrayIndexOutOfBoundsException in oracle.jdbc.driver.DynamicByteArray class.	RHEL
OS PROVISIONING		
221199 C	ProLiant Scripting Toolkit for Linux x64 - 2015.06.0 is using an old version of the Toolkit.	Linux
192472 C	Upgrade fails as the item is already available in the Library.	Linux
193783 C	OS Build Plan fails reboot on Satellite Facility.	
194888	SA Client does not allow "." in Kickstart file.	
202061 C	OSSequenceService.configureAutomaticProvisioningRule API is not scalable.	
207208 C	OSBP disables security logging during build.	Linux
207496 C	Server boots into unprovisioned servers pool with incorrect NIC information.	
208369 C	MBC hostname changes to default after hardware registration.	
208875 C	RHEL 7 OS Provisioning fails when custom kickstart config file has lines that begin with percent (%) character.	
210046 C	Conrep fails to save hardware configuration when provisioning ProLiant Gen9 servers.	Linux
212959	OSBP does not prompt for the server to be assigned to a Customer.	Linux
215444 C	MBC fails when attempting to provision a server.	Linux
217645 C	RedHat7 provisioning fails when % post script contains % include statement.	Linux
218931 C	OSBP - A connection to the agent cannot be established.	Linux
188842 C	Twist error : ilo auto registration fails silently.	Independent
220007 C	Proliant Build Plans fail because the ZIP packages have not been updated to work with the Service OS.	Linux
221529 C	WinPE runs in issue when it cannot download DHCPOptions.ini from tftp server with Infoblox DHCP server.	Linux
225057 C	Unattend xml file injection script is mangling the DNS-Client component.	
PATCHING		
190753 C	CBT fails to import certain Windows patches.	

191519 C	Unable to determine True Patch Availability Status when download URL changes with same checksum and exists on word.	Linux
191652 C	populate-opsware-update-library can take a long time to process the MS patch DB and provides no feedback to user.	
191974 C	The solpatch_import tool fails to import solaris 10 patches with the error "SSL routines:SSL3_GET_RECORD:wrong version number".	
194286 C	Deleted windows patches can have their UNITS record put into a hybrid DELETED/ACTIVE state if wsusscn2.cab is imported before the UNITS record is GC'ed.	
199011	MBSA .cab import via populate-opsware-update-library script takes too long.	Windows
201369 C	Previously installed common multi binary can cause false "Installed Patch".	Windows
203190 C	HP-UX depots might be downloaded multiple times, wasting disk space and potentially causing timeouts.	
203191 C	HP-UX bundles are not reported in compliance.	
202022 C	Unable to import Solaris 10 01/13 (Update 11) Patch Bundle into SA.	
203364 C	CBT message should be clear when certain Windows patches are not uploaded.	Linux
204623 C	Could not uninstall windows patch KB3018238 via SA.	Linux
188279 C	PatchBundle unittype adding changed unit_file_name and unit_loc format. This caused CBT import/exports to fail leaving customers with unusable data.	Linux
207414 C	solpatch_import displays "NameError: global name 'srcpath' is not defined".	
SOFTWARE MANAGEMENT		
221154 C	rhn_import fails to download packages.	
184160	RedHat Linux patching spends significantly longer time in App Compliance phase, with much higher overall CPU usage on Database server and larger LCREP_DATA tablespace consumed.	Independent
156243 C	Server scripts fail with the following Error Code: wayscripts.lockFailed.	Linux
192225 C	rhn_import fails with error "RHN SSO Login Failed".	
194285 C	A unit uploaded with the same unit_loc of a previously deleted unit can result in a REALM_UNITS leak.	

183704 C	Core content synchronization is not working as expected.	Linux
201463 C	Support for RHEL 7 packages using rhn_import tool.	
195137	SA global shell API connections bypassing UNIX security.	Independent
203674 C	"User doesn't have install software permissions" on scheduled jobs if one of the server is decommissioned and the server ID does not exist.	Independent
203847 C	uln_import is not able to register user/servers in SA versions higher than 10.02. "AttributeError: sendall" error.	
204068	Provide option to skip importing superseded MBSA patches.	Windows
205299 C	opsware.agent_reach.check_reachability does not handle errors for remote commands.	Linux
207396 C	Email from a remediation job contains a stack trace regardless of the job status.	
207715	Difficult to troubleshoot Satellite upgrade failure due to upstream Satellite being temporarily disconnected from mesh.	
210407	Upgrade rpm gives conflict error while deploying package.	
211056 C	zypper integration fails if there is no rpm-python package available on the managed server.	SLES
212106 C	Automatic communications test jobs fail to run due to "STALE" status.	
189055 C	Software policy with AUO (Automatic Update Ordering) disabled cannot be changed.	
214703 C	Transactions should be handled and not dropped if the sending vault's file system is full.	Linux
215460	Getting "Unexpected error: ValueError: unconverted data remains: UTC" when using redhat_import to import RHEL7 label.	
217393 C	populate-opsware-update-library ignores errors during extraction of wsusscn2.cab upload.	Linux
220969 C	Vault concurrency problem around fetching transactions from the database.	HP-UX
224486 C	suse_manager_import should use the API to determine the package download URL.	Linux
USABILITY		
194765	When using a file copy operation from the Device Explorer, an update of the device name occurred instead while trying to select	Linux

	target server.	
208925 C	NGUI threads spawned to retrieve device summary data can overload the twist.	Linux
VIRTUALIZATION		
202047 C	Downloading an updated existing cookbook does not get the latest one if tsunami is used.	Independent
214224	Oracle performance problems on certain queries with optimizer_ index_cost_adj set to 20.	Linux

Documentation information

This section discusses documentation information for this release.

Access to SA documentation

All SA documentation is available as individual documents, or as a bundle in the SA 10.50 Documentation Library on the HPE Software Support website. This site allows access to guides, release notes, support matrices, and white papers for all current and past SA releases. You can also access the current Documentation Library from the SA client online help: select Help > Help Contents, Index and Search.

> **Note:**
> The HPE Software Support website requires an HPE Passport, which you can create once you access the site. After signing in, click the Search button and begin filtering documentation and knowledge documents using the filter panel. To download the documents, click the go link.

Once you download documents to your local drive:

- Unzip the files.
- Use docCatalog.html (which provides an indexed portal to the downloaded documents in your local directory) to find individual documents.

> **Note:**
> Some of the white papers, although released in earlier patches, are still relevant to this release. You will also receive notification, if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (Server Automation 10.50)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!